Política de Gerenciamento de Vulnerabilidades ePatches

Dados do documento
ID Interno EVDOC: 51-8529
Data do documento: 2023-01-25
Versão do documento: 2023-01-25
Fluxo de aprovação EVDoc: 52-8529-02
Sigla / Denominação: PGVP
Empresa: EVSolid (Aqui Referida como EV)
Responsável PGVP: DSI (Departamento de Segurança da Informação)

Sumário

1 – OBJETIVO

Esta política tem como objetivo estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da organização.
A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de tecnologia da informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

2 – ESCOPO

Esta política de gerenciamento de vulnerabilidades se aplica aos sistemas e ativos informacionais da EV, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

Os serviços de TI críticos da EV devem ser formalmente elencados pelo DSI daEV.

A tabela de serviços e processos críticos ficará disponível como material complementar a esse documento por entender que tais serviços ou processos podem surgir, modificar ou se extinguirem com certa facilidade, e assim sendo, essa política ficará mais dinâmica e atualizada sem riscos ao processo como um todo.

O DSI é responsável por elaborar, manter e fazer cumprir a política de gerenciamento de Vulnerabilidades.

Exceções
Pode ocorrer que alguns ativos de informação da EV não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta política deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções da EV.

Público
Esta política de gerenciamento de vulnerabilidades (PGV) da EV se aplica a indivíduos responsáveis pela gestão e a indivíduos que utilizam qualquer ativo de informação da rede ou computadores em nome da EV. Além disso, a presente política se aplica a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos da EV.

3 – TERMOS E DEFINIÇÕES

AMEAÇA – Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.

ANÁLISE DE VULNERABILIDADES – Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas.

ATIVOS DE INFORMAÇÃO – Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

BANCO DE DADOS – Coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.

CVE (Common Vulnerabilities and Exposures) – Vulnerabilidades e Exposições Comuns.

CVSS (Common Vulnerability Scoring System) – Sistema comum de pontuação de vulnerabilidade.
HOST – Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall).

ID CVE – Identificação para um CVE específico.

GERENCIAMENTO DE VULNERABILIDADE – Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.

GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO – Processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

GESTOR DE SEGURANÇA DA INFORMAÇÃO – Responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

LOG (REGISTRO DE AUDITORIA) – Registro de eventos relevantes em um dispositivo ou sistema computacional.

NTP (Network Time Protocol) – Protocolo de Tempo para Redes.

PATCH – Uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente.

PENTEST – Acrônimo de teste de penetração (penetration test).

REMEDIAÇÃO – O ato de corrigir uma vulnerabilidade ou eliminar uma ameaça.

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.

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.

TESTE DE INVASÃO – Metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante.

TESTE DE PENETRAÇÃO (PENTEST) – Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pelo órgão ou entidade.

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.

4 – DECLARAÇÕES DA POLÍTICA

Os sistemas e os dispositivos conectados à rede da EV, sejam eles próprios ou aqueles em processo de desenvolvimento e suporte por terceiros, devem passar periodicamente por varreduras em busca de vulnerabilidades que possam representar um risco para a infraestrutura e os dados sensíveis da EV.

Novos aplicativos/sistemas construídos pela equipe de desenvolvimento da EV ou de terceiros devem ser verificados no que concerne a vulnerabilidades antes de serem implantados no ambiente de produção.

4.1 – Processo de gerenciamento de vulnerabilidades (PGV)

1. Um processo de gerenciamento de vulnerabilidades (PGV) deve ser criado, implementado, mantido e aplicado na EV.
2. O processo deve conter a implementação de mecanismos para obter informações oportunas sobre vulnerabilidades técnicas dos sistemas e ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.
3. O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, como a ativos que compõe a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros.
4. O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV.
5. O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para a EV.
6. O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.
7. A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.
8. As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo DSI e suas medições devem ser apresentadas a cada seis meses.

4.2 Mapeamento de ativos de informação

1. Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches para determinar qual marca, modelo e versão de equipamento de hardware, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de software são usados na EV.
2. O mapeamento de ativos de informação deve ser atualizado a cada 6 meses ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades da EV

4.3 Detecção de vulnerabilidades

1. As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.
2. As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.
3. Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.
4. A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que a EV deve cumprir e os riscos associados aos ativos avaliados.
5. As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou

uma combinação de ambos.

6. Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.
7. Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades.
8. As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos.
9. O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade da EV ou pelo menos uma vez por ano, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal da EV.
10. A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.
11. A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

4.4 Elaboração e manutenção dos relatórios

A equipe de gerenciamento de vulnerabilidades deve elaborar relatórios após cada ciclo de detecção para auxiliar a EV a entender e mensurar as vulnerabilidades existentes.

Os resultados da varredura devem passar por análise da equipe de gerenciamento de vulnerabilidades com o dispositivo ou gerenciador de rede para que possíveis falsos positivos possam ser identificados e eliminados.

Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade. A equipe de gerenciamento de vulnerabilidades deve adotar métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS. 26.A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; autoridade de numeração CVE; e tipo de vulnerabilidade.

O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.

Todas as versões do relatório devem ser remetidas ao gestor(a) de segurança de informação.

4.5 Banco de dados de vulnerabilidades

Deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de software, que precisam ser aplicadas aos sistemas e ativos informacionais da EV.

O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.

O banco de dados deve ser atualizado regularmente com as informações mais recentes. As novas

vulnerabilidades devem ser adicionadas ao banco de dados tão logo forem descobertas.

É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de patches. Isso ajuda a identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.

As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

4.6Priorização e Correção de vulnerabilidade

O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio da EV.

As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados abaixo.

Nível de Severidade	Prazo de correção	Descrição do risco
Muito crítico (6)	Até 2 dias	Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.
Crítico (5)	Até 30 dias	Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.
Alto (4)	Até 45 dias	Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.
Médio (3)	Até 90 dias	Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (2)	Até 120 dias	Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas.
Muito baixo (1)	Até 180 dias	Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.

Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo estabelecido no item 35, a

equipe de gerenciamento de vulnerabilidade deve enviar uma “solicitação de renúncia” ao departamento/coordenação de segurança da informação da EV. A solicitação deve conter as seguintes informações:

- Detalhes do sistema ou ativo.
- Descrição detalhada da vulnerabilidade.
- Avaliação de risco que justifique a não correção imediata.
- A justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido.
- Detalhes dos controles existentes (se houver).
- Novo prazo de correção.
- Plano de ação da remediação (obedecendo o novo prazo de correção).

A decisão de aceitar ou rejeitar a solicitação de renúncia deve ser tomada pelo(a) departamento/coordenação de segurança da informação da EV, com base na avaliação de risco apresentada. Se a solicitação de renúncia for aceita, a vulnerabilidade deve ser monitorada continuamente, pautado pelo plano de ação apresentado devendo ser corrigida assim que possível.
Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

4.7 Das exceções

O objetivo é garantir que as exceções à política de gerenciamento de vulnerabilidades sejam tratadas de forma transparente e consistente, minimizando os riscos potenciais e protegendo adequadamente os ativos de informação da organização.

1. Para os ativos de informação da EV não contemplados por esta política em função de dificuldades técnicas ou obrigações contratuais e normativas ou outras razões legítimas, as exceções deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções da EV.
2. A lista de exceções de ativos de informação deve ter validade de um ano, devendo ser revisada após esse período.

4.8 Dos registros de logs

1. Identificar quais eventos dos ativos de informação devem ser registrados, com base nos requisitos regulatórios, nas melhores práticas e nos objetivos da EV.
2. Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.
3. As configurações referentes a ativos de informação devem incluir configurações de log para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.
4. Definir procedimento para análise de logs, como ferramentas de análise e correlação, para identificar possíveis ameaças e vulnerabilidades.
5. Uma revisão dos arquivos de registro (logs) deve ser conduzida pelo menos a cada seis meses.
6. Os arquivos de registro (logs) devem ser protegidos contra adulteração e acesso não autorizado ou vazamento.
7. Registros de logs dos sistemas e ativos informacionais classificados como críticos devem ser

mantidos por pelo menos 3 anos, tempo suficiente para cumprir os requisitos regulatórios e permitir a detecção de ameaças passadas.
8. Monitorar regularmente os registros de logs para identificar quaisquer tentativas de exploração de vulnerabilidades.
9. Registros de log devem ser excluídos de forma segura, garantindo que os registros sejam completamente apagados sem deixar vestígios ou dados remanescentes.

4.9 Comunicação da ocorrência de vulnerabilidades e correções.

1. As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.
2. As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (Pentest) e verificação das definições de configuração.

4.10 Implementação e verificação das correções de vulnerabilidades

1. As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de logs.
2. Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de software.
3. Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do processo de gestão de mudanças para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

4.11 Dos serviços em nuvem ou de terceiros

1. Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas.
2. Terceiros devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades (PGV). Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

5 – CONCLUSÃO

A política de gerenciamento de vulnerabilidades e patches, mesmo tendo um carácter técnico deve ser reconhecida como uma das mais importantes por todos os colaborares da EV. A operação dessa política é bem técnica mas o seu entendimento ajuda os membros das demais áreas a munir a criticidade dos dados ao DSI e ao Departamento de TI.