POLÍTICA DE GERENCIAMENTO DE VULNERABILIDADE – PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

MARÇO – 2023

Sumário

1 – OBJETIVO

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle de Privacidade e Segurança da Informação da Vector. Ter uma gestão contínua de Vulnerabilidades, desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da empresa, a fim de remediar e minimizar a janela de oportunidade para atacantes.

2 – ABRANGÊNCIA

Esta Política de gerenciamento de vulnerabilidades se aplica aos sistemas e ativos informacionais da Vector, incluindo funcionários, gestores, prestadores de serviços, fornecedores e parceiros.
O departamento de TI da Vector é responsável por elabora, manter e fazer cumprir essa Política.

3 – REFERÊNCIAS

Essa política de vulnerabilidade tem como referência os seguintes documentos:

- Política de Segurança da Informação;
- Política Complementar da Segurança da Informação – Cibernética;
- Plano de Continuidade de Negócios.

4 – DEFINIÇÕES

- Ameaça – Conjunto de fatores externos com o potencial de causarem dano para um sistema ou empresa.
- 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 empresa.
- 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.
- HOST – Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall).
- Gerenciamento de Vulnerabilidade – Processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades.
- Gestão de 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.
- 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 empresa.
- 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 empresa.
- 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.

5 – DIRETRIZES

5.1 – Processo de Gerenciamento de Vulnerabilidades

1. Esse processo de Gerenciamento de Vulnerabilidades deve ser implementado, mantido e aplicado na Vector;
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 Vector 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 Vector, como a ativos que compõe a rede da empresa, 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 dessa política;
5. O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz Vector;
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 pela TI e suas medições devem ser apresentadas a cada seis meses.

5.2 – Mapeamento de Ativos de Informação

A TI deve fazer 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 Vector.

O mapeamento de ativos de informação deve ser atualizado periodicamente ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades da Vector.

5.3 – Identificação de Vulnerabilidades

Essa política de vulnerabilidades de rede estabelece procedimentos para identificar e avaliar regularmente as vulnerabilidades nas redes de computadores da Vector. Isso inclui a realização de varreduras de vulnerabilidades utilizando ferramentas automatizadas, como scanners de vulnerabilidades, bem como a análise de resultados e a revisão de informações de segurança de fornecedores confiáveis.

5.4 – Avaliação de Riscos

Essa política de vulnerabilidades de rede inclui procedimentos para avaliar o risco associado a cada vulnerabilidade identificada. Isso envolve a análise da gravidade das vulnerabilidades, sua exploração potencial e o impacto que podem ter nos sistemas e dados da Vector. Com base nessa avaliação de risco, as vulnerabilidades podem ser classificadas em diferentes níveis de prioridade para a aplicação de medidas de mitigação adequadas.

5.5 – Patching e Atualizações

A política de vulnerabilidades de rede defini os procedimentos para a aplicação de patches e atualizações de segurança em sistemas e dispositivos de rede. Isso incluir a definição de prazos para a instalação de patches, a priorização com base na gravidade das vulnerabilidades e a definição de responsabilidades claras para garantir que as atualizações sejam aplicadas de forma oportuna e eficaz.

5.6 – Gerenciamento de Configuração

Essa política de vulnerabilidades de rede aborda o gerenciamento de configuração dos sistemas e dispositivos de rede, incluindo a definição de configurações seguras e a implementação de medidas para garantir que as configurações adequadas sejam mantidas. Isso pode envolver o uso de padrões de configuração seguros, o controle de acesso aos dispositivos de rede, a autenticação forte e outras práticas de gerenciamento de configuração.

5.7 – Monitoramento e Detecção de Ameaças

A política de vulnerabilidades de rede pode incluir a implementação de práticas de monitoramento e detecção de ameaças, como a análise de registros de eventos de segurança, a implantação de sistemas de detecção de intrusões (IDS) ou sistemas de prevenção de intrusões (IPS), e outras medidas para identificar atividades suspeitas ou comportamentos anormais que possam indicar a exploração de vulnerabilidades.

5.8 – Classificação da Varredura

1 – Intenção ou finalidade da varredura:

- Varredura de rede de segurança – essa é uma varredura realizada pela TI para identificar vulnerabilidades e pontos fracos na rede, com o objetivo de fortalecer a segurança e proteger os sistemas contra ameaças.
- Varredura de rede de teste de penetração – também conhecida como teste de penetração ou “pentesting”, essa é uma varredura realizada pela TI com o objetivo de avaliar a segurança da rede identificando e explorando vulnerabilidades, a fim de fornecer feedback detalhado sobre a eficácia das medidas de segurança existentes.

2 – Tipo de técnica de varredura:

- Varredura de rede ativa – essa varredura, são enviados pacotes de dados ativamente para a rede, com o objetivo de identificar portas abertas, serviços em execução, sistemas operacionais ou outras informações relevantes.
- Varredura de rede passiva – essa varredura não são enviados pacotes de dados ativamente para a rede, mas sim informações são coletadas passivamente a partir do tráfego de rede existente, com o objetivo de identificar informações sobre a rede.

3 - Contexto da varredura:

- Varredura de rede interna – é realizada dentro da rede interna da Vector.
- Varredura de rede externa – é realizada a partir de fora da rede da Vector.

5.9 – Priorização e Correção de Vulnerabilidades

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 Vector.
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
Crítica	De 2 (dias)	Vulnerabilidades classificadas como críticas são aquelas que a Vector definiu que terá um alto impacto na segurança do sistema ou rede, com potencial para serem exploradas remotamente e causarem danos graves. Elas podem permitir a execução remota de código, acesso não autorizado completo ao sistema, ou comprometimento total de dados sensíveis, foi definido pela TI que essas

		vulnerabilidades exigem uma ação imediata e prioridade máxima na aplicação de medidas de mitigação.
Alta	Até 30 (dias)	Vulnerabilidades classificadas como altas pelo Vector são as que têm um alto potencial de serem exploradas e causarem danos significativos à segurança do sistema ou rede. Embora não sejam tão graves quanto as vulnerabilidades críticas, elas ainda exigem uma atenção e ação imediatas para aplicação de medidas de mitigação. Elas podem permitir acesso não autorizado limitado, divulgação parcial de informações sensíveis, ou interrupção parcial dos serviços.
Média	Até 90 (dias)	Vulnerabilidades classificadas pela Vector como médias têm um potencial de exploração e impacto moderados na segurança do sistema ou rede. Elas podem permitir acesso não autorizado limitado, divulgação parcial de informações não críticas, ou causar interrupções menores nos serviços. Embora não sejam tão urgentes quanto as vulnerabilidades críticas ou altas, ainda requerem ação para aplicação de medidas de mitigação.
Baixa	Até 120 (dias)	Vulnerabilidades classificadas pela Vector como baixas têm um baixo potencial de exploração e impacto na segurança do sistema ou rede. Elas podem ter um impacto mínimo na confidencialidade, integridade ou disponibilidade dos dados e serviços, e podem não exigir uma ação imediata, mas ainda requerem monitoramento e consideração para a aplicação de medidas de mitigação.
Informativa	Até 180 (dias)	Essa categoria é geralmente usada pela Vector para informações sobre vulnerabilidades que não representam uma ameaça significativa à segurança do sistema ou rede, mas fornecem informações úteis sobre a configuração ou estado do sistema para fins de monitoramento e melhoria contínua da segurança.

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 com autorização da direção, com base no processo de aceitação de risco.

6 – DOS REGISTROS DE LOGS

O registro de logs é uma prática importante no controle de vulnerabilidades de redes, pois pode ajudar a identificar atividades suspeitas ou maliciosas que possam indicar tentativas de exploração de vulnerabilidades. Os logs são registros detalhados das atividades do sistema, como eventos de autenticação, tentativas de acesso, atividades de rede, erros e outras informações relevantes.

Por isso, a Vector faz os registros de logs na sua rede.

Aqui estão algumas práticas que Vector faz relacionadas ao registro de logs no controle de vulnerabilidades de redes:

- Ativar o registro de logs: Certificar-se de que os logs estão ativados em todos os sistemas e dispositivos relevantes, incluindo servidores, firewalls, roteadores, switches e outros dispositivos de rede.
- Configurar logs detalhados: Configurar os logs para registrar informações detalhadas, incluindo registros de autenticação, logs de eventos de segurança, logs de tráfego de rede e logs de sistema. Quanto mais detalhados forem os registros, maior será a capacidade de detectar atividades suspeitas.
- Armazenar logs em local seguro: Armazenar os logs em um local seguro e protegido contra acesso não autorizado. Os logs devem ser protegidos contra exclusão acidental ou intencional, e o acesso aos logs deve ser restrito apenas a pessoal autorizado.
- Monitorar e analisar logs regularmente: Estabelecer uma rotina de monitoramento e análise dos logs para identificar atividades suspeitas ou eventos anômalos que possam indicar tentativas de exploração de vulnerabilidades. O uso de ferramentas de análise de logs e soluções de gerenciamento de eventos e informações de segurança pode ser útil nesse processo.

- Responder a eventos de log suspeitos: Ter procedimentos e políticas em vigor para responder a eventos de log suspeitos, incluindo a investigação, análise e resposta a possíveis explorações de vulnerabilidades. Isso pode envolver a tomada de ações corretivas, como a aplicação de correções de segurança, a implementação de medidas de mitigação ou a notificação de incidentes de segurança.
- Realizar auditorias de logs: Realizar auditorias regulares dos logs para garantir a integridade e a precisão dos registros. Isso pode ajudar a identificar possíveis lacunas na configuração dos logs ou atividades suspeitas que podem ter passado despercebidas.
- Manter registros de logs por um período adequado: É importante manter os registros de logs por um período adequado, em conformidade com as políticas de retenção de dados da organização e os requisitos regulatórios aplicáveis. Isso pode ser útil para fins de investigação e análise de incidentes futuros.

Em resumo, o registro adequado de logs é uma prática importante no controle de vulnerabilidades de redes, permitindo a detecção precoce de atividades suspeitas e a resposta eficaz a possíveis explorações de vulnerabilidades.

7 – CORREÇÕES

Segue algumas práticas definidas pela TI para as correções de vulnerabilidades:

- Verificar a aplicação das correções;
- Realizar testes de penetração;.
- Monitorar a ocorrência de novas vulnerabilidades;
- Atualizar a documentação.

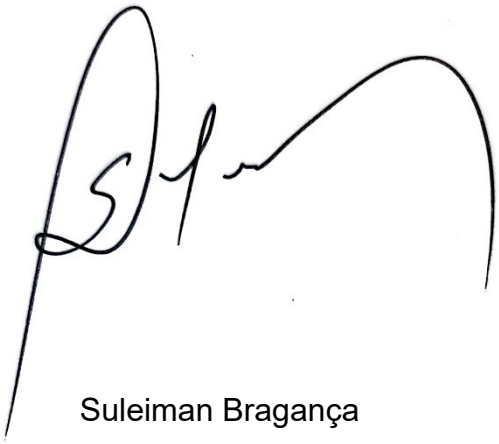
8 – CONSCIENTIZAÇÃO E TREINAMENTO

A conscientização e treinamento dos colaboradores, parceiros e fornecedores em relação à importância da segurança de rede, boas práticas de segurança cibernética e ações a serem tomadas em caso de identificação de vulnerabilidades ou ameaças é primordial. Por isso a Vector incluir treinamentos regulares, campanhas de conscientização, e a promoção de uma cultura

9 – VIGÊNCIA

A presente Política Técnica de Gerenciamento de Vulnerabilidades da Vector terá vigência da data de sua publicação até ser revogado pela empresa. Essa política pode sofrer alterações conforme análise da TI. Caso sofra alguma alteração será comunicada em treinamento para todos da Vector.

Barueri, março de 2023



Suleiman Bragança
CEO