**POLÍTICA DE GESTÃO DE VULNERABILIDADES**

1. **INTRODUÇÃO**

Aqui na **Stark Industries** desenvolvemos uma nova metodologia para execução de testes de segurança (Pentests) sob demanda e totalmente escalável. Assim, elaboramos esta Política de Segurança da Informação e Cyber Security (Política) para reafirmar o compromisso que temos com a adoção das melhores práticas de segurança da informação e proteção dos dados dos nossos clientes.

1. **OBJETIVO**

O objetivo desta política é delinear os requisitos para que todos os sistemas sejam verificados em busca de vulnerabilidades e que todas as descobertas sejam relatadas, analisadas e rastreadas até a resolução de acordo com os SLAs aqui definidos.

1. **AUDITORIAS**

As seguintes diretrizes serão aplicadas na Stark Industries no momento que estiver sendo realizado testes e auditorias de segurança:

* O escopo dos testes técnicos de auditoria deve ser acordado e controlado;
* Os testes de auditoria devem ser limitados ao acesso somente leitura a software e dados;
* O acesso que não seja somente leitura só deve ser permitido para cópias isoladas de arquivos do sistema, que devem ser apagados quando a auditoria for concluída, ou receber proteção adequada se houver uma obrigação de manter tais arquivos sob requisitos de documentação de auditoria;
* Os testes de auditoria que possam afetar a disponibilidade do sistema devem ser realizados fora do horário comercial;
* Todos os acessos devem ser monitorados e registrados para produzir uma trilha de auditoria.

1. **ANÁLISE DE VULNERABILIDADES E TESTES DE SEGURANÇA DE INFRAESTRUTURA**

A verificação e identificação das vulnerabilidades da **Stark Industries** são realizadas por:

* Bitdefender Gravityzone
* Scoutsuite

Além disso, verificações periódicas de segurança dos sistemas da **Stark Industries** são feitas usando uma combinação de ferramentas externas de teste de vulnerabilidade comercial e de código aberto, incluindo:

* Probely
* Snyk

1. **TESTE DE INVASÃO**

Os testes de invasão são realizados regularmente por um terceiro independente.

As descobertas de uma verificação de vulnerabilidade e/ou teste de invasão são analisadas pelo responsável pela segurança, juntamente com a TI e a engenharia, conforme necessário, e relatadas por meio do processo definido na próxima seção.

1. **RELATÓRIO, RASTREAMENTO E CORREÇÃO DE VULNERABILIDADE DE SEGURANÇA**

A **Stark Industries** utliza um processo de controle de vulnerabilidades usando Jira. Os registros das descobertas são retidos indefinidamente.

1. **RETENÇÃO DAS INFORMAÇÕES**

* Após a identificação de uma vulnerabilidade (incluindo vulnerabilidade em software, sistema ou processo), um ticket Jira é criado;
* A descrição da descoberta deve incluir mais detalhes, sem qualquer informação confidencial, e um link para a fonte;
* A descoberta receberá um nível de prioridade no Jira.

1. **CLASSIFICAÇÃO DE PRIORIDADE/GRAVIDADE E SLAs**

Em um esforço para remediar rapidamente as vulnerabilidades de segurança, os seguintes cronogramas foram implementados:

|  |  |  |  |
| --- | --- | --- | --- |
| **Prioridade** | **SLA** | **Definição** | **Exemplos** |
| **CRÍTICA** | Imediatamente após a detecção por meio de hotfix | Vulnerabilidades que causam um escalonamento de privilégios na plataforma de não privilegiado para administrador, permitem execução remota de código, roubo financeiro, acesso não autorizado/extração de dados confidenciais etc. | Vulnerabilidades que resultam em execução remota de código, como desvio de autenticação vertical, SSRF, XXE, injeção de SQL, desvio de autenticação de usuário. |
| **ALTA** | Dentro de 24 horas | Vulnerabilidades que afetam a segurança da plataforma, incluindo os processos que ela suporta. | Ignorar autenticação, XSS armazenado, algum CSRF dependendo do impacto. |
| **MÉDIA** | Dentro de 30 dias | Vulnerabilidades que afetam vários usuários e exigem pouca ou nenhuma interação do usuário para serem acionadas. | XSS reflexivo, referência direta a objetos, redirecionamento de URL, algum CSRF dependendo do impacto. |
| **BAIXA** | Dentro de 30 dias (Arrumar assim que possível) | Problemas que afetam usuários individuais e exigem interação ou pré-requisitos significativos (MitM) para serem acionados. | Falhas comuns, informações de depuração, headers. |

1. **RESOLVENDO UMA VULNERABILIDADE**

* A descoberta deve ser atribuída ao proprietário responsável pelo sistema ou pacote de software;
* Todas as descobertas devem ser abordadas de acordo com o SLA estabelecido;
* Nenhum software deve ser implantado em produção com descobertas CRÍTICAS ou ALTAS não\* resolvidas, a menos que uma Exceção esteja em vigor (veja abaixo);
* Uma descoberta pode ser resolvida por:
  + Fornecendo uma correção/mitigação válida;
  + Determinando como um falso positivo;
  + Documentando uma exceção aprovada.

1. **FECHANDO UMA VULNERABILIDADE**

* O cessionário deve fornecer uma resolução válida (veja acima) e adicionar um comentário à conclusão;
* A descoberta deve ser reatribuída ao Relator ou a um membro da equipe de segurança para validação;
* Após a validação, a descoberta pode ser marcada como concluído (fechado) pelo Reporter;
* Antes que a descoberta possa ser marcada como fechada pelo relator, a correção deve ser implantada em um ambiente de desenvolvimento e ter uma data de lançamento prevista para implantação na produção anotada no ticket.

1. **EXCEÇÕES**

* Uma Exceção pode ser solicitada quando uma solução viável ou direta para uma vulnerabilidade não estiver disponível. Por exemplo, uma versão do pacote que contém a correção não é suportada no sistema operacional específico em uso;
* Uma solução alternativa (também conhecida como controle de compensação) deve estar em vigor para resolver a vulnerabilidade original, de modo que o risco seja mitigado. O controle compensatório pode ser técnico ou de processo ou uma combinação de ambos;
* Uma exceção deve ser aberta na forma de um ticket Jira;
* O problema de exceção deve fazer referência à descoberta original adicionando um link de problema ao problema da descoberta;
* Cada exceção deve ser revisada e aprovada pelo Diretor de Segurança e pelo proprietário do ativo impactado.

1. **ATUALIZAÇÕES**

A Política de Segurança Cibernética e demais políticas devem ser revisadas, no mínimo, a cada dois anos.

1. **COMUNICAÇÃO**

Em caso de dúvida, questão ou preocupação em relação a esta Política, entre em contato através de **security@starkindustries.com.br**.

1. **REVISÕES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versão** | **Data** | **Revisão** | **Aprovação** | **Conteúdo Revisado** |
|  |  |  |  |  |

1. **INFORMAÇÕES DE CONTROLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versão** | **Código do Documento** | **Área** | **Status** | **Confidencialidade** |
| 1.0 |  |  |  |  |