Imprimir

Ver anotações 0

FOCO NO MERCADO DE TRABALHO

ANÁLISE DE VULNERABILIDADE E *PENTEST*

Emilio Tissato Nakamura

O QUE É *PENTEST*?

O teste de intrusão é um método que avalia a segurança de um sistema, determina “se” e “como” um agente de ameaça pode obter um acesso não autorizado a ativos que afetam um ambiente e identifica vulnerabilidades nos controles de segurança dos componentes do sistema.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

As vulnerabilidades são os pontos explorados pelos agentes de ameaça em ataques. As plataformas *web* e móvel que serão desenvolvidas são compostas por diferentes elementos ou ativos, os quais podem conter vulnerabilidades e, portanto, devem ser identificadas e tratadas. Ativos como sistema operacional, componentes de infraestrutura ou bibliotecas de *software* de terceiros também podem conter vulnerabilidades que devem ser eliminadas. As aplicações em si, que serão desenvolvidas, também podem inserir vulnerabilidades no sistema e, portanto, o desenvolvimento do sistema deve considerar a segurança em todo o seu ciclo de vida.

Assim, a gestão de vulnerabilidades da empresa deve prever a descoberta, priorização de ativos, avaliação, relatório, remediação e verificação da remediação em todos os ativos do sistema, incluindo os de terceiros e os que serão implementados. Como o ambiente do sistema muda constantemente, e novas vulnerabilidades são sempre descobertas, a gestão de vulnerabilidades deve ser implementada para acompanhar o dinamismo dos ambientes web e móvel.

Ver anotações

Dentre os diferentes testes de segurança que podem ser realizados, o plano é adotar os mais completos, o que foi indicado pela avaliação de riscos. Como os testes mais completos são os que requerem mais recursos, incluindo o tempo, o planejamento é fundamental.

O plano prevê, assim, testes de segurança a serem realizados internamente e com o ponto de vista externo, do agente de ameaça.

Os testes internos fazem parte do ciclo de vida de desenvolvimento de *software*, com atividades de segurança sendo feitas nas fases de definição, especificação, desenvolvimento, implantação e manutenção das plataformas *web* e móvel.

A análise de vulnerabilidades no código-fonte, a *Static Analysis Security Testing* (SAST), será feita por sua equipe. A SAST complementará outras atividades de segurança e privacidade importantes durante o desenvolvimento, antes da implantação:

- Treinamento da equipe em segurança e privacidade.
- Revisão de políticas e padrões de segurança e privacidade.
- Uso de métricas para medir a segurança e privacidade das plataformas web e móvel;
- Revisão dos requisitos de segurança, incluindo mecanismos como gerenciamento de usuários, autenticação, autorização, confidencialidade de dados, integridade, contabilidade, gerenciamento de sessão, segurança no transporte, segregação em camadas, conformidade com legislação e padrões.
- Revisão da especificação e arquitetura.
- Criação e revisão integrada dos modelos UML.
- Criação e revisão do modelo de ameaças.
- Execução simulada do código.
- Teste do gerenciamento de configuração.

Ver anotações

Outro teste de segurança a ser realizado antes da implantação, com a plataforma *web* e móvel em execução, é a *Dynamic Analysis Security Testing* (DAST). Normalmente, a análise dinâmica não provê as informações que a análise estática provê, mas detecta elementos sob o ponto de vista do usuário, como os ativos, funções, pontos de entrada e outros.

Após a implantação do sistema, o plano é a contratação de uma empresa especializada em *pentest*, para complementar os testes feitos pela sua própria equipe. A empresa contratada fará o teste de caixa preta, com uma visão total do agente de ameaça, enquanto a sua equipe fará o teste de caixa branca, que faz sentido pela sinergia existente com os outros testes de segurança da fase de desenvolvimento, com o acesso ao código-fonte, documentação e diagramas. Estes testes serão complementados pelas atividades necessárias no ambiente de produção:

- Revisão do gerenciamento operacional.
- Verificação das mudanças.

Ver anotações

AVANÇANDO NA PRÁTICA

PROJETO NOVO COMEÇANDO, COM SEGURANÇA

A empresa em que você trabalha teve sucesso com investidores e, por isso, foi aprovado um orçamento para o desenvolvimento de um novo projeto, que é um novo sistema de gerenciamento de energia solar. Você faz parte da equipe e sua responsabilidade como gestor de segurança e privacidade é grande, pois os investidores e executivos da empresa sabem que os ativos envolvidos controlam grandes recursos financeiros que são manipulados pelo sistema. Focando nos testes de segurança, apresente o plano para que a implantação do sistema seja feita de uma forma segura.

RESOLUÇÃO

O ciclo de vida de desenvolvimento de software deve incluir a segurança e privacidade, com a definição dos pontos em que os processos de segurança serão feitos.

O treinamento de desenvolvimento seguro para toda a equipe, visando minimizar a incorporação de vulnerabilidades, é apoiado por políticas, padrões e documentações.

A segurança e privacidade fazem parte dos requisitos de todo o sistema, com requisitos específicos e é realizada revisão da especificação e arquitetura sob essa perspectiva.

Com o uso de modelos de ameaças e alinhamento quanto ao funcionamento de todo o sistema e as implicações de segurança e privacidade, a codificação é acompanhada com a execução simulada e a revisão do código implementado.

São realizadas análises estáticas (SAST) e dinâmicas (DAST) antes da implantação do sistema.

Ver anotações

E o *pentest* é realizado no ambiente de homologação uma vez, e outra vez no ambiente de produção, junto dos testes de gerenciamento de configuração.

Após a implantação, é feita a revisão de gerenciamento operacional e as verificações das mudanças, que incluem novas análises de vulnerabilidades.

Novos *pentests* (caixa cinza) são feitos periodicamente, a cada bimestre. Para tanto, uma credencial de usuário será disponibilizada para a empresa especializada contratada.

Ver anotações 0