PHISHX

A importância do ciclo de desenvolvimento seguro

Desenvolvimento seguro

Expostas a ameaças cada vez maiores dentro do mundo virtual, as organizações precisam estar preparadas para se proteger e mitigar os possíveis riscos. Quando falamos de desenvolvimento de sistemas, grande parte das organizações possuem processos bem definidos. Porém, muitas equipes de desenvolvimento ainda não percebem a segurança como parte importante do processo.

Um sistema inseguro pode colocar qualquer organização em risco, suas vulnerabilidades podem ser exploradas por criminosos, comprometendo as operações. Dessa forma, é importante pensar em integrar a segurança durante todo o ciclo do desenvolvimento. Então, vamos falar um pouco sobre SDLC, sigla em inglês para Ciclo de Desenvolvimento Seguro.

Por que o SDLC é importante?

Um ciclo de desenvolvimento seguro, SDLC, é uma estrutura para que todo o processo de construção de um sistema, ou aplicativo, seja feito de forma segura. Ele integra testes de segurança durante todas as fases de desenvolvimento. Isso quer dizer que, um ciclo de desenvolvimento seguro transforma a preocupação com segurança em algo contínuo, detectando falhas precocemente e reduzindo os riscos globais dos negócios.

Segundo especialistas, problemas encontrados nas fases iniciais de desenvolvimento custam menos para serem reparados do que aqueles encontrados após a implementação do sistema. Dessa forma, o SDLC evita a necessidade de alterações após a entrega do produto, diminuindo os custos de desenvolvimento e reduzindo suas vulnerabilidades. Assim, é importante que o projeto já siga procedimentos seguros desde o início, tornando as iniciativas de segurança um padrão para o desenvolvimento.

Como funciona?

De maneira geral, um ciclo de desenvolvimento seguro envolve a integração de testes de segurança dentro dos processos já existentes. As atividades incluem análise da arquitetura, revisão frequente do código e construção de teste de penetração antes do lançamento.

Existem diversos exemplos de modelos SDLC, eles descrevem práticas que as organizações podem adotar para intensificar a segurança de seus sistemas. Profissionais que desenvolvem ou testam softwares, podem adotar algumas práticas que melhoram a segurança das organizações.

Boas práticas

Atualmente, grande parte das estratégias de segurança digital das organizações não podem deixar de passar pelas pessoas. Elas são parte importante da mitigação de riscos e precisam estar conscientizadas sobre a importância da segurança da informação. Assim, é preciso que os profissionais que atuam dentro das áreas de desenvolvimento estejam atualizados sobre as práticas seguras de codificação e estruturas disponíveis para a segurança de softwares.

Também é importante medir os riscos da arquitetura desde o início do desenvolvimento, e sempre considerar a segurança ao planejar e construir testes. Além disso, o uso de ferramentas de digitalização de código para análise estática e dinâmica, além de testes interativos de segurança de aplicativos, trazem mais segurança para o processo.

Vá além

É muito importante que as organizações desenvolvam iniciativas para abordarem de forma mais estratégica o ciclo de desenvolvimento seguro. Para isso, é importante analisar a efetividade dos processos e políticas de segurança existentes, e se eles deixam lacunas. Os gestores também podem criar iniciativas de segurança de software para alcançar estratégias mais efetivas de segurança.

Se você já segue um SDLC seguro, esteja sempre em busca de melhorias. Avaliar os programas desenvolvidos e comparar com o de outras organizações pode auxiliar a manter os processos atualizados e sem vulnerabilidades.