**+O**

**Próximos Passos para Organizações**

**Comece Agora o seu Programa de Segurança de Aplicações**

A Segurança de Aplicações já não é opcional. Ataques cada vez mais frequentes e pressão para seguir a regulamentação exigem que as organizações estabeleçam um programa efetivo de segurança das aplicações. Dado o grande número de aplicações e linhas de código que já estão em produção, muitas organizações estão a enfrentar dificuldades em controlar o número elevado de vulnerabilidades. A OWASP recomenda que as organizações estabeleçam um programa de segurança de aplicações para ganhar visibilidade e melhorar a segurança dos seus portfolios de aplicações. Obter segurança de aplicações requer que várias partes da organização trabalhem em conjunto e de maneira eficiente, incluindo segurança e auditoria, desenvolvimento de software, gestão de negócio e executiva. É necessário que a segurança seja visível, para que todos os envolvidos possam entender a postura da organização em relação à segurança de aplicações. É preciso também focarem-se em atividades e resultados que realmente ajudem a melhorar a segurança da corporação através da redução do risco com um bom custo/beneficio. Algumas das atividades chave de um programa eficaz para a segurança de aplicações incluem:

|  |  |
| --- | --- |
| Iniciando | •Estabelecer um programa de segurança de aplicações e estimular sua adoção. •Conduzir uma análise de diferenças de capacitação, e comparar a sua organização com outras semelhantes, definindo áreas chave para melhorias e um plano de execução.  •Obter aprovação da gestão de topo e estabelecer uma campanha de consciencialização em segurança de aplicações para toda a organização de TI. |
| Abordagem de Portfolio Baseada em Risco | •Identificar e estabelecer prioridades no portfolio de aplicações usando uma perspectiva de risco.  •Criar um modelo de avaliação de risco em aplicações para medir e prioritizar as aplicações do portfolio.  •Estabelecer directivas de segurança com o fim de definir a cobertura e o nível de rigor necessários.  •Estabelecer um modelo comum de classificação de riscos aliado a um conjunto consistente de fatores de impacto e probabilidade que reflitam a tolerância de risco da organização. |
| Ativar com uma fundação sólida | •Estabelecer um conjunto de politicas e normas que sejam uma base para segurança de aplicações a ser seguida por todas as equipas de desenvolvimento.  •Definir um conjunto comum de controlos de segurança reutilizáveis que complementem as políticas e normas, contendo orientações de uso para as fases de projeto e desenvolvimento.  •Estabelecer um currículo de formação em segurança de aplicações obrigatório e direcionado às diversas funções de desenvolvimento e tópicos existentes. |
| Integrar Segurança aos Processos Existentes | •Definir e integrar implementações de segurança e atividades de verificação nos processos de desenvolvimento e operação existentes. As atividades incluem Modelação de Ameaças, Projeto Seguro e Revisão, Codificação e Revisão de Código com Segurança, Testes de Intrusão, e Correção. •Oferecer especialistas e serviços de suporte para as equipas de desenvolvimento e projeto para obter êxito nos processos. |
| Oferecer Visibilidade para a Gestão | •Gerir usando métricas. Efetuar melhorias e decisões de investimento baseadas nas métricas e análises dos dados capturados. Métricas incluem aderência às atividades e práticas seguras, vulnerabilidades introduzidas, vulnerabilidades mitigadas, abrangência da aplicação, densidade de defeitos por contagem de tipo e instância, etc.  •Analisar dados das atividades de implementação e verificação procurando por causas raiz e padrões de vulnerabilidade com o fim de conduzir as melhorias estratégica e sistematicamente em toda a empresa. |