ATHENA
SOLUÇÕES INTELIGENTES

GUIA SEGURANÇA DE APLICAÇÃO

Adote as melhores práticas e processos em sua empresa

ATHENA
SOLUÇÕES INTELIGENTES

Sumário

ATHENA
SOLUÇÕES INTELIGENTES

Introdução

Você já ouviu falar em **segurança de aplicações**? Esse processo é bastante comum na área da tecnologia e trata-se de um conjunto de ações que visam construir, lançar e manter as aplicações, sempre adotando as melhores práticas de Desenvolvimento Seguro. Ao contrário do que muitos pensam, a segurança de aplicações não é apenas a realização de testes mas, sim, um processo que funciona de forma contínua.

Estima-se que 90% dos aplicativos que são desenvolvidos tenham vulnerabilidades e isso é alarmante. Por isso que investir em segurança é tão importante e necessário. Além disso, com ambientes cada vez mais complexos, híbridos e totalmente na nuvem, muitas empresas trabalham com praticamente todas as aplicações legadas e terceiras. Isso porque existe uma grande utilização de códigos pré-desenvolvidos para acelerar o processo de desenvolvimento. Por um lado adianta o trabalho mas também pode trazer uma série de falhas e problemas.

Em meio a esse cenário, como garantir que a sua esteira de DevOps e sua análise de aplicações terceiras avaliem potenciais vulnerabilidades? A resposta está na utilização de plataformas de automação!

ATHENA
SOLUÇÕES INTELIGENTES

Afinal, o que é segurança de aplicação?

Segundo **pesquisas do Gartner**, 75% dos ataques cibernéticos realizados no mundo exploram as **vulnerabilidades das aplicações**. É por isso que o investimento emsegurança é tão importante e necessário.

Ao terem os dados acessados por criminosos, por exemplo, as empresas podem ter impactos financeiros e econômicos. Além disso, os danos de imagem também ocorrerão e a organização pode perder a confiança de seus clientes. Cabe lembrar ainda que já está valendo, no Brasil, a Lei Geral de Proteção de Dados (LGPD), que penaliza as organizações que vazarem dados de terceiros, como clientes e funcionários. Vale ressaltar que tais vazamentos podem ocorrer em decorrência de falhas de segurança nas aplicações.

Os valores das multas da LGPD podem chegar a 2% do faturamento total da empresa, com limite de R$ 50 milhões.

ATHENA
SOLUÇÕES INTELIGENTES

Conceito e um pouco da história da segurança de aplicação

O termo **segurança de aplicação** começou a ser utilizado ainda na época da Segunda Guerra Mundial, quando ocorreu o primeiro ataque hacker da história.

Na ocasião, a Bombe, uma ferramenta desenvolvida pelos poloneses, foi utilizada para decifrar dados de códigos secretos do governo da Alemanha. Desde então, os militares de praticamente todo o mundo passaram a tomar mais cuidado com as aplicações que utilizam, evitando que dados sensíveis sejam acessados pelos inimigos.

A partir da década de 1990, quando a computação começou a ser muito mais utilizada no meio empresarial, as empresas também passaram a se preocupar com isso e as tecnologias se desenvolveram.

ATHENA
SOLUÇÕES INTELIGENTES

Shift-left: o fluxo base da segurança de aplicação

Praticamente todos os pesquisadores e especialistas no desenvolvimento de **softwares** e de **aplicações** concordam que o fluxo shift-left é a base para a segurança de uma aplicação.
Trata-se de um modelo de desenvolvimento em que as aplicações são desenhadas a partir de uma orientação horizontal, da esquerda para a direita. Observe o gráfico abaixo:

A ideia do fluxo shift-left é fazer com que a segurança já seja pensada na ponta, ou seja, no início do desenvolvimento de uma aplicação.

ATHENA
SOLUÇÕES INTELIGENTES

Sendo assim, ao criar um sistema ou aplicativo, 5 passos devem ser seguidos. São eles:

1 Requirement (Requisitos)

Esta é a etapa de desenvolvimento das aplicações em que se deve pensar nos requisitos a serem cumpridos para que elas sejam seguras.
Para isso, uma série de testes pode ser realizada, inclusive para conhecer o perfil do público que utilizará a aplicação.

2 Design

Na etapa do Design, as aplicações são desenhadas e projetadas de acordo com os requisitos que foram estabelecidos anteriormente.
Testes de usabilidade e experiência, ou chamados UI e UX, também podem ser realizados nesse momento.

3 Coding (Codificação)

A etapa da Codificação diz respeito à elaboração dos códigos de programação que permitem o funcionamento da aplicação.
Nesse momento, os programadores devem sempre elaborar códigos com boas práticas de segurança, para que não sejam vulneráveis a ataques ou qualquer outro tipo de cibercrime.

ATHENA
SOLUÇÕES INTELIGENTES

Testing (Testando)

4

A etapa do testing é bastante simples. Trata-se da realização de testes do projeto desenvolvido. Os testes podem ser realizados internamente pela equipe desenvolvedora e, também, por usuários aleatórios para verificar como o recurso desenvolvido impacta os usuários comuns.

Maintenance (Manutenção)

5

Engana-se quem pensa que as atividades de segurança de aplicação se encerram quando o produto é colocado no ar. Depois que os usuários estiverem utilizando o recurso, inicia-se a etapa manutenção da aplicação. O objetivo é que possíveis vulnerabilidades sejam identificadas. Assim, o processo entra num ciclo de melhoria contínua.

ATHENA
SOLUÇÕES INTELIGENTES

Diferença entre segurança de aplicação e vulnerability management

Embora tenham algumas semelhanças, os processos são diferentes e saber quais são as competências de cada um deles é fundamental para que seja possível atuar em cada situação. O **vulnerability management** é um processo que visa avaliar, relatar e corrigir vulnerabilidades cibernéticas em endpoints, cargas de trabalho e sistemas. Em resumo, na infraestrutura.

> *"Vulnerabilidade é uma fraqueza de um ativo ou grupo de ativos, que pode ser explorada de acordo com uma ou mais ameaças."*
>
> **International Organization of Standardization (ISO)**

A segurança de aplicação, por sua vez, vai além do vulnerability management. O processo, como explicado, é contínuo e se inicia ainda no desenvolvimento da solução. Ao contrário do vulnerability management, que visa identificar e corrigir vulnerabilidades, o papel da segurança de aplicação é nem sequer deixar que elas ocorram ou, pelo menos, reduzir essa possibilidade de forma significativa.

ATHENA
SOLUÇÕES INTELIGENTES

Tipos de vulnerabilidades

Existem diferentes tipos de vulnerabilidades que podem gerar ameaças cibernéticas para as empresas, mas destacaremos aqui as duas principais:

Vulnerabilidades no código

As vulnerabilidades de código são aquelas que se referem à segurança do próprio software ou aplicação. Esse tipo de vulnerabilidade, portanto, é uma falha de segurança no código, que cria um potencial risco de comprometer a segurança da aplicação. Por meio de uma vulnerabilidade no código, um agente de ameaça pode tirar proveito da situação para anexar um ponto de acesso e roubar dados sigilosos da empresa, por exemplo.

Vulnerabilidades na operação

São aquelas que não estão relacionadas à aplicação em si, mas sim à forma como elas são utilizadas.
Os erros por conta de desatenção, falta de conhecimento (uma senha fraca, por exemplo) ou até mesmo atitudes mal-intencionadas dos colaboradores da empresa são exemplos de vulnerabilidades na operação.
É por isso que a adoção de políticas internas de segurança é tão importante para as organizações. E um bom plano de segurança de aplicação deve considerar ambos os tipos de vulnerabilidades para os negócios.

HCL AppScan: referência em segurança de aplicação

Como solução para a segurança de aplicação, a **Athena Soluções Inteligentes** realiza a implementação de HCL APPScan.
Trata-se de uma tecnologia de testes de segurança SAST, DAST e IAST, que permite um processo de desenvolvimento mais seguro, sem perder eficiência da esteira de DevOps.

Com uma infinidade de linguagens abrangidas e a possibilidade de ser usado em ambientes complexos, o HCL APPScan possibilita a seus clientes testar aplicações próprias e terceiras, e expor eventuais vulnerabilidades de forma automatizada e rápida.

Além disso, é possível comprar avaliações pontuais e atender a demandas de análises de segurança em aplicações sem grande investimento, abarcando necessidades contínuas e pontuais.
Sem dúvida, esta é uma das melhores soluções de segurança de aplicação do mercado e vale a pena buscar por mais informações sobre o assunto!

ATHENA
SOLUÇÕES INTELIGENTES

Conclusão

Os **desenvolvedores de aplicações**, assim como os gestores de TI das empresas que as utilizam, precisam estar sempre cientes de questões sobre segurança. Além disso, eles precisam ser treinados continuamente para que saibam lidar com as tecnologias atualizadas e que todas as etapas do desenvolvimento ocorram de forma segura.

ATHENA
SOLUÇÕES INTELIGENTES

Conheça a Athena Soluções Inteligentes

Somos uma **consultoria com foco em GRC | IRM –** Governança, Riscos e Compliance, Segurança da Informação e LGPD, formada por profissionais certificados e altamente experientes na condução de serviços e implementação de soluções próprias e de parceiros.

Utilizamos soluções robustas, líderes no quadrante mágico do Gartner e com ampla presença na nossa região.

Em nosso portfólio – Athena Professional Services – atuamos fortemente com Implementação de Soluções, Serviços Pós Implementação de Soluções, Auditorias e Gap Analysis, Treinamentos e Consultoria, com clientes de todos os segmentos de mercado em todo o país.

Nosso desafio é construir soluções inteligentes e inovadoras para ofertar ao mercado o que há de mais moderno e atualizado em GRC | IRM, Segurança da Informação e LGPD.

www.athenasolucoes.com

ATHENA
SOLUÇÕES INTELIGENTES

ACESSE NOSSAS
REDES SOCIAIS: