Como utilizar o Pentest na cibersegurança do seu negócio

20 de setembro de 2022 Trade Technology
Cibersegurança, Compliance, Segurança da Informação
0 Comentários

É inegável que o aumento do uso da tecnologia no dia a dia das organizações trouxe inúmeros benefícios para o crescimento dos negócios, como a integração de sistemas e a automatização de processos, por exemplo.

Ao mesmo tempo, trouxe também uma maior preocupação com a exposição dos sistemas computacionais e dos dados corporativos às ameaças virtuais, que vem aumentando.

Segundo o relatório da Kaspersky, os ataques cibernéticos a empresas brasileiras cresceram 41%, de janeiro a abril de 2022, em comparação com o mesmo período do ano anterior.

Por isso, manter uma postura preventiva às ameaças através do uso de ferramentas e práticas, como a cibersegurança é essencial para as empresas, que visam se beneficiar das vantagens da tecnologia, sem colocar em risco a sua segurança.

Neste artigo, te explicamos como utilizar o Pentest ou teste de instrusão, um dos métodos utilizados para identificar vulnerabilidades e proteger os ambientes das empresas.

Leia também: Cibersegurança: proteção em primeiro lugar

O que é o Pentest ou “teste de intrusão”?

> O Teste de Intrusão, mais conhecido como Pentest, é um método de prevenção a ameaças, utilizado para avaliar a segurança de um sistema computacional ou de uma rede.

É um exercício, onde especialistas em cibersegurança simulam cenários reais de ataque em ambientes de empresa, utilizando ferramentas e metodologias avançadas para explorar e identificar vulnerabilidades que poderiam facilitar invasões.

Dessa forma, as políticas de segurança da empresa poderão ser ajustadas de acordo com as falhas encontradas, aumentando a confiabilidade da infraestrutura de TI e a segurança da empresa contra possíveis ataques.

Tipos de Pentest

Os testes de intrusão costumam incluir todas as partes da infraestrutura como redes, dispositivos conectados, entre outros, e até mesmo elementos de segurança física e externos da empresa.

Black Box
Nesse modelo o trabalho todo o trabalho é realizado “às cegas”. Não é fornecida nenhuma informação acerca do sistema, suas características ou estruturação, cabendo à equipe desvelar estes detalhes para planejar seu ataque. É o mais parecido com um ataque externo.

Grey box
A equipe de testers detém algum conhecimento sobre a infraestrutura ou sistema alvo. Essa informação pode estar relacionada a sua estrutura, organização, segurança ou até mesmo hábitos e costumes de seus operadores humanos.

White Box
O pentester tem acesso a praticamente toda a infraestrutura antes de planejar o ataque. Isso significa que podem planejar seu trabalho

considerando todas as características do sistema. Quando pertinente, isso representa uma grande vantagem para a equipe, que economiza tempo e recursos. Os testes white box são o modelo de pentesting padrão e tendem a ser bastante confiáveis.

Etapas do Pentest

1. **Alinhamento:** na etapa inicial é definido o escopo dos testes, os objetivos, expectativas, abordagens, regras de engajamento (o que pode e não pode) e riscos relacionados. Além do tipo de Pentest mais adequado para as necessidades e realidade da empresa (WhiteBox, BlackBox ou GreyBox); \

2. **Coleta de informações:** diversas técnicas são utilizadas nessa parte do processo para identificar todas as informações públicas disponíveis e que possam ser usadas no Pentest;
3. **Varredura e enumeração:** é realizado um escaneamento para identificar os ativos tecnológicos disponíveis ou definidos no escopo e suas vulnerabilidades. Classificando-os conforme seu potencial de risco e ameaças a organização;
4. **Exploração:** com as informações obtidas na varredura são realizadas tentativas de acesso à rede. Onde técnicas e ferramentas são aplicadas com o objetivo de explorar as vulnerabilidades identificadas e penetrar o sistema;
5. **Pós-exploração:** após adentrar o sistema é preciso encontrar formas de aumentar o nível de acesso, coletar mais informações, e garantir a sustentação da acessibilidade;
6. **Documentação:** a última etapa realizada é a elaboração de um relatório com todas as informações levantadas com o Pentest, como vulnerabilidades, explorações e falhas na segurança. Além da descrição dos impactos e nível de criticidade de cada achado, também é apresentado uma visão geral do processo com recomendação e medidas de correção e mitigação para serem implantadas.

Como utilizar o Pentest na cibersegurança do seu negócio

O ideal é que o Pentest faça parte de um conjunto maior de práticas voltadas para a segurança e a gestão de vulnerabilidades das empresas. Devendo ser utilizado de forma preventiva e contínua, ou sempre que um sistema receber adições à infraestrutura, atualizações de software, hardware ou firmware.

O teste é indicado para todas as empresas, especialmente do setor público, mercado financeiro, grandes corporações e companhias, que coletam, armazenam ou manipulam dados sensíveis, e necessitam de um ambiente seguro e praticamente inviolável para trabalhar.

Além disso, o Pentest possui diversas funções e benefícios importantes como:

- **Identificar o nível de exposição de uma empresa a ameaças externas e internas;**
- **Testar a eficácia de todos os mecanismos de proteção e capacidade interna de resposta a incidentes de segurança;**
- **Analisar riscos e impactos de um ataque real;**
- **Apontar soluções e gerar relatórios com as medidas e estratégias de correção para serem implementadas em todo o ambiente da organização;**
- **Atender a compliance e requisitos impostos pela lei da LGPD;**
- **Aumentar o nível de maturidade de segurança e credibilidade perante o mercado;**

A aplicação do Pentest pode ser realizada internamente, no caso da empresa contar com uma área de TI e segurança capacitada para isso. Do contrário, o serviço pode ser terceirizado por empresas de TI como a Trade Technology.

Nossa área de consultoria em Segurança da Informação conta com um time de profissionais especialista em cibersegurança e LGPD e oferece o serviço de Pentest nos formatos: **Externo, Interno, Engenharia Social e DDos (Denial of Service)**.
Utilizando metodologias avançadas como Penetration Testing Execution Standard e OWASP.

Além disso, a Trade Technology oferece soluções inovadoras em Governança de Dados, Infraestrutura de TI e Desenvolvimento de Softwares de Inteligência Cognitiva, e possui parceria com os principais players do mercado de Tecnologia.
Fale com nossos profissionais e descubra a melhor solução em TI para o seu negócio!

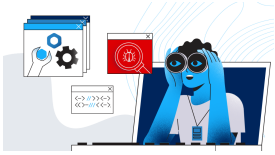
cibersegurança | como identificar vulnerabilidades em TI | DDos | engenharia social | gestão de vulnerabilidades | lgpd | métodos da cibersegurança | outsourcing TI | OWASP | Penetration Testing Execution Standard | pentest | pentester | segurança da informação | simulação de ataque hacker | teste de intrusão

Compartilhe

Twitter | Facebook | LinkedIn | Email

Trade Technology

Artigos relacionados



A importância de realizar a gestão de vulnerabilidades na sua empresa

Na era da informação digital, os ataques

Os benefícios do backup corporativo para seu negócio!

Existem diversas situações que podem causar a perda de

Ransomware: perigo à vista para pequenas empresas

Pequenas empresas não costumam se preocupar muito com