CONSULTORIA

PENTEST

*O **Pentest** (Penetration testing), também chamado de Teste de Invasão ou Intrusão, simula um ataque real a uma aplicação, rede ou sistema buscando identificar vulnerabilidades que possam ser exploradas de modo a comprometer o ambiente.*

A técnica pode ser realizado em aplicações web, aplicações mobile, redes, redes sem fio, cloud e outros sistemas.

OBJETIVO_

O principal objetivo de um Pentest é identificar falhas que possam ser exploradas por um atacante, causando comprometimento ao ambiente tecnológico da organização. O Pentest também pode ser utilizado para testar os controles implementados e as habilidades da equipe de segurança da informação. Através do Pentest a organização adquiri a capacidade de escolher conscientemente seus investimentos em segurança.

A QUEM SE DESTINA_

Boa parte das organizações podem ser consideradas alvos potenciais de cibercriminosos, sejam elas entidades governamentais ou empresas privadas, sem distinção de porte ou o segmento. Por este motivo, o Pentest é indicado para empresas que visam proteger seus dados e compreendem os reflexos negativos associados a perda ou vazamento de informações.

BENEFÍCIOS_

- *Aumenta o nível de segurança ;*
- *Satisfaz necessidades de compliance PCI 3.x, FFIEC, HIPAA;*
- *Legado em segurança para time de tecnologia;*
- *Evita gastos para remediar incidentes de segurança;*
- *Preserva a imagem da marca.*
- *Rápido retorno sobre o investimento*

ENTREGÁVEIS_

Relatório

_ Resumo executivo.

_ Vulnerabilidades e classificações de riscos identificados.

_ Etapas detalhadas da correção de riscos.

_ Ativos e dados comprometidos durante a avaliação.

Remediation Testing

_ Um novo penetration testing sobre as vulnerabilidades listadas no relatório deve ser executado após a empresa sinalizar a correção.

ostec
Segurança digital de resultados

METODOLOGIA_

White-box, Black-box, Grey-Box.

Testes executados in-loco e remotamente, de acordo com a necessidade evidenciada.

1 Reconnaissance_

Descoberta de dados cruciais sobre o alvo, fornecendo a base para a execução de um Pentst personalizado.

2 Enumeration & Vulnerability Scanning_

Uso de ferramentas de verificação de vulnerabilidades e análise manual para identificar e mapear falhas de segurança.

3 Attack and Penetration_

Escalada de privilégios e identificação dos riscos técnicos e impacto total no negócio.

4 Reporting & Documentation_

Relatório com: resumo executivo, vulnerabilidades e classificação de riscos, detalhamento sobre a correção dos riscos e resumos dos ativos/dados comprometidos durante a avaliação.

5 Remediation Testing_

Execução de um Pentest sobre as vulnerabilidades listadas no relatório entregue na fase de Reporting.

Standars & Metodology_

- Open Web Application Security Project (OWASP);
- Open Source Security Testing Methodology (OSSTMM);
- Penetration Testing Execution Standard (PTES).

ostec
Segurança digital de resultados

+55 48 3052.8500

www.ostec.com.br
contato@ostec.com.br

MAIS INFORMAÇÕES

Acesse o site e obtenha informações completas sobre este e outros serviços.