excelia

Pentesting

Identifique vulnerabilidades hoje, para evitar ataques amanhã.

A digitalização das empresas trouxe consigo a necessidade de proteger os sistemas contra possíveis ciberataques. Estes ataques podem causar interrupções nos serviços, perdas financeiras significativas e fugas de informação sensível. Neste contexto, a cibersegurança assume-se como um ativo estratégico para qualquer organização, independentemente da sua dimensão ou setor de atividade, garantindo a continuidade operacional, a proteção de dados críticos e a confiança de clientes, parceiros e stakeholders.

Recorrer a um serviço de pentesting é fundamental para identificar vulnerabilidades antes que sejam exploradas por cibercriminosos.

Este serviço simula ataques reais, para revelar vulnerabilidades nos sistemas da organização. Ao antecipar-se a estas ameaças, a organização consegue aplicar medidas corretivas atempadamente, reforçando a segurança e protegendo os seus ativos digitais contra possíveis ciberameaças.

Identificando vulnerabilidades internas

Fatores como erros humanos, acessos não controlados ou falta de formação podem criar fragilidades de segurança. Por isso, é crucial realizar testes de penetração para detetar e corrigir tanto as vulnerabilidades externas como as internas, garantindo assim uma proteção abrangente contra todos os tipos de ameaças.

Benefícios Principais

Identificação de Vulnerabilidades:
Deteção de falhas de segurança antes que sejam exploradas por cibercriminosos.

Resposta a Incidentes:
Avalie e melhore a reação da sua equipa perante ataques.

Cumpra com a Legislação:
Cumpra com as novas diretivas como DORA e NIS2, e garante a conformidade com diretivas consolidadas como GDPR, HIPAA e PCI-DSS.

Proteja os Dados:
Salvaguarde a informação crítica da sua empresa.

Economize Custos:
Reduza custos ao prevenir ataques decorrentes de falhas de segurança.

Proteção da reputação:
Evite vulnerabilidades que possam comprometer a confiança dos seus clientes e parceiros estratégicos.

excelia

Tipos de Pentesting

Por nível de acceso

Caixa Branca
Acesso total ao códig
e aos sistemas internos.

Caixa Negra
Simula um ataque externo, sem qualquer informação prévia sobre os sistemas.

Caixa Cinza
Acesso parcial às informações internas.

Por objetivo

Redes

Aplicações web

Dispositivos móveis

Fases do Pentesting

1. **Planeamento e preparação**
   Definição do âmbito e objetivos.
2. **Reconhecimento**
   Recolha de informações.
3. **Análise de vulnerabilidades**
   Identificação de fraquezas.
4. **Exploração**
   Simular ataques para avaliar o impacto e o nível de risco.
5. **Pós-exploração**
   Obter informações adicionais e explorar outras possíveis vulnerabilidades.
6. **Relatório e recomendações**
   Entrega de documentação detalhada com conclusões e propostas de ação claras.

Serviços relacionados

Cybersecurity Consulting - CISO as a Service - Data Security - Cloud Security - Network Security - Application Security - Vulnerability Assessment - Endpoint Security - Threat Intelligence

Por que excelia

Equipa Especializada:
A nossa equipa é composta por profissionais com sólida experiência e certificações reconhecidas no setor da cibersegurança.

Abordagem Personalizada:
Metodologias e ferramentas adaptadas às necessidades especificas do seu negócio.

Relatório Claro e Ação:
Entregamos um relatório completo com s descrição das vulnerabilidades e recomendações claras e fáceis de implementar.

Suporte Contínuo:
Apoiamos a sua equipa em todas as fases do processo. Oferecemos suporte contínuo para ajudar a sua equipa a lidar com as vulnerabilidades identificadas.

info@excelia.com - www.excelia.com