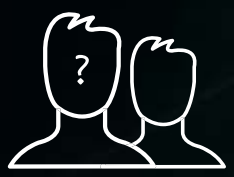
CYBERSOC

ETHICAL HACKING

Serviços de EH confiáveis para manter os sistemas corporativos seguros



Social Engineering Testing

Social Engineering Testing

Um Social Engineering Test é um conjunto de técnicas utilizadas para avaliar a segurança dos recursos e ativos da organização a partir do ponto de vista da matéria de segurança das pessoas dentro de nossa organização.

Esse conjunto de técnicas identifica as vulnerabilidades existentes em nível de conscientização e conhecimento sobre diferentes vetores de ataques orientados às pessoas dentro de nossa organização. Especificamente, busca-se, além da identificação, a exploração das vulnerabilidades relacionadas à fraude com essas pessoas e, dessa maneira, observa-se o impacto real sobre a organização por meio dessa.

Este tipo de serviço é realizado interna e externamente, onde, internamente se busca identificar e explorar as vulnerabilidades que sejam visíveis num cenário com acesso aos recursos e ativos da organização, enquanto externamente, acontece através de diversas fraudes como campanhas de phishing, chamadas para a empresa, entrega de dispositivos maliciosos, etc

Objetivos principais

- ✓ Obter uma fotografia do estado da segurança da organização em um momento determinado.
- ✓ Visualizar sua empresa a partir do ponto de vista do atacante, localizando fraquezas, vulnerabilidades e pontos de acesso não autorizados, antes que os atacantes o façam.
- ✓ Comprovar o verdadeiro impacto das vulnerabilidades em seu ambiente particular.
- ✓ Comprovar se o nível de proteção existente condiz com a política de segurança estabelecida
- ✓ Comprovar a efetividade de suas medidas de proteção, políticas e processos de detecção de intrusos e resposta a incidentes.
- ✓ Descobrir vulnerabilidades a partir de mudanças nas configurações da infraestrutura.
- ✓ Acompanhar a aplicação de patches e correções de vulnerabilidades na organização.

Por que realizar um Social Engineering Testing?

- ✓ Para conhecer o estado da segurança de uma organização (especialmente se nunca foi realizada uma auditoria dessas características)., relacionado e direcionado particularmente à conscientização e capacitação de nossos empregados.

- ✓ Para estabelecer um ponto de partida e começar a gerir a segurança da organização.
- ✓ Para constituir um ciclo de revisão e melhoria para a segurança de forma contínua. Para tentar minimizar todo tipo de ameaça

As etapas associadas a este serviço são:

- ✓ Reconhecimento da organização ou objetivo.
- ✓ Análise e detecção de possíveis vulnerabilidades de Social Engineering Testing.
- ✓ Exploração de vulnerabilidades associadas.
- ✓ Montagem e apresentação de relatórios

Todas estas etapas são orientadas e baseadas nos possíveis vetores de exploração que possam ser realizados dentro do serviço.

Relatórios

Neste serviço, são gerados 2 entregáveis ou relatórios que ajudam e orientam o cliente no processo de correção de vulnerabilidades.

O primeiro deles, o **relatório executivo**, descreve o nível de risco da empresa sem entrar em detalhes técnicos, evidenciando os problemas por meio de conceitos claros e gráficos.

O segundo relatório, o **relatório técnico**, direcionado para a área técnica da empresa, visa ajudar a equipe de TI a solucionar os problemas detectados.

Neste relatório, são mostradas todas as evidências dos testes executados de tal forma que todas as tarefas sejam escaláveis e transparentes para o cliente.


ESET CYBERSOC