NÚCLEO DE DEFESA CIBERNÉTICA

CATÁLOGO DE SERVIÇOS

PENTEST DE REDE (INTERNA): o objetivo deste teste é identificar e testar toda a superfície de ataque interno da organização. Este serviço aumenta a postura geral de segurança da organização, identificando os hosts que podem ser usados como apoios para os saltos laterais em uma rede que devem ser remediados.

PENTEST DE BORDA (EXTERNA): o objetivo deste teste é identificar e testar toda a superfície de ataque externo da organização. Este serviço aumenta a postura geral de segurança da primeira linha de defesa da organização.

ENTEST DE CLOUD (NUVEM): o objetivo é avaliar ambientes de nuvem. Analisando microsserviços baseados na nuvem, armazenamentos de dados na memória, funções sem servidor, malhas Kubernetes e contêineres, além de identificar e testar aplicativos nativos e nativos da nuvem. Um teste de penetração de um ambiente de nuvem hospedado por um terceiro provedor de serviços como Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), etc. Este tipo de engajamento é muitas vezes emparelhado com um teste de penetração interna para determinar se o acesso ao ambiente interno pode ser usado para obter acesso ao ambiente de nuvem e pivô em outras localizações.

PENTEST PCI: o objetivo é para identificar e testar toda a superfície de ataque da organização que pode afetar a segurança dos dados do titular do cartão (CHD) ou do cartão titular Data Environment (CDE). O objetivo deste teste é realizar um teste completo de todos os serviços disponíveis expostos em sistemas que armazenam, processam ou transmitem CHD têm conectividade a esses sistemas, ou de outra forma impactar a segurança do CHD (por exemplo, sistemas de autenticação, sistemas de gerenciamento de configuração, etc.).

VALIDAÇÃO DE SEGMENTAÇÃO: o objetivo é avaliar a eficácia de quaisquer controles de segmentação de rede (por exemplo, firewalls, listas de controle de acesso, etc.) usados para reduzir o escopo do PCI DSS ao tentar conectar e acessar o ambiente de dados do titular do cartão (CDE) a partir de vários segmentos de rede destinados a ficar fora do escopo para conformidade com PCI DSS. Além de outros setores que devem estar isolados dentro de uma rede, como por exemplo aplicativo e banco de dados.

VERIFICAÇÃO DE INFRAESTRUTURA: o objetivo principal é verificar os ativos, as políticas de atualização de firmwares e senhas, acessos para configuração e backup entre outros.

EXPLORAÇÃO DE VULNERABILIDADES (WEB, MOBILE, CLOUD): o objetivo é levantar as vulnerabilidades conhecidas entre os hosts testados em etapas anteriores e indicar as possíveis correções que devem ser aplicadas.

ENGENHARIA SOCIAL (*VISHING*, *PHISHING* E *PHYSICAL*): o objetivo é avaliar a capacidade para prevenir e reagir a um ataque direcionado contra a organização bem como o nível de conscientização de segurança dos usuários. *Vishing* envolve usuários sendo chamados por telefone e atraídos a divulgar informações confidenciais ou ajudando involuntariamente um invasor para comprometer os sistemas. *Phishing* envolve usuários sendo contatados por e-mail e atraídos a divulgar informações confidenciais ou ajudando involuntariamente um invasor para comprometer os sistemas. O objetivo de um teste de penetração física é avaliar a capacidade de prevenir e reagir a uma intrusão física. Isso inclui disfarçar o invasor como legítimo ocupante ou terceiro autorizado na esperança de obter uma compreensão avançada dos controles de segurança atuais da instalação.

PERÍCIA FORENSE DIGITAL: tem como intuito determinar a materialidade, dinâmica e autoria de ilícitos associados ao âmbito da computação, tendo a identificação e o processamento de evidências como provas materiais do crime.

ANÁLISE DINÂMICA DE APLICAÇÕES: tem como objetivo realizar uma análise comportamental envolvendo desde a execução do código, monitorando seu comportamento, até a interação e os efeitos sobre o sistema infectado, normalmente feito na modalidade de *white box*.

ANÁLISE ESTÁTICA DE CÓDIGO FONTE: tem por objetivo analisar estaticamente o código fonte da aplicação por meio de software especializado para tal fim, visando evidenciar problemas, para que possam ser corrigidos com o máximo de foco, resultando em maior eficiência no processo de melhoria de qualidade.

ANÁLISE DE MALWARE: é o processo de execução de malware e análise de sua funcionalidade e comportamento. O objetivo é entender exatamente o que o malware faz durante a execução. Inclui o monitoramento de processos, entradas de registo e monitoramento de rede para determinar o malware.

CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES: auxiliar os clientes na escolha de ferramentas tecnológicas usadas para acelerar e facilitar as metas corporativas. Dessa forma, ao aplicar a TIC, a empresa tem a possibilidade de automatizar processos, otimizar a aprendizagem, reduzir gastos, etc.

CONSULTORIA EM SEGURANÇA CIBERNÉTICA: verificar a capacidade de detectar e responder a ataques cibernéticos. Verificar a arquitetura de segurança física e apontar suas vulnerabilidades. Checar as políticas de segurança que regem a estratégia geral de segurança da organização e propor melhorias. Desenhar a solução de segurança necessária para lidar adequadamente com os objetivos de negócios da organização.

Ficamos à disposição para esclarecer quaisquer dúvidas quanto aos serviços adicionais realizados pela COOPERX.

COOPERX Brasil
Endereço: Setor Comercial Sul 502 Bloco C, S/N, Sala 37 – Asa Sul
Brasília, Distrito Federal - CEP 70330-530
E-mail comercial@cooperx.com.br
Web: www.cooperx.com.br WhatsApp: (061) 99338-3106