Iniciando no mundo da cibersegurança

Cassiano Peres

DIO Tech Education Analyst

cassiano-dio

peres-cassiano

Objetivo Geral

Neste curso vamos abordar os tópicos fundamentais para iniciar no vasto mundo da cibersegurança, focando em termos, conceitos e práticas de cibersegurança.

Pré-requisitos

É desejável um conhecimento prévio em programação, redes de computadores e sistemas operacionais.

Percurso

Etapa 1 Cibersegurança, o que é?

Etapa 2 O que é hacking?

Etapa 3 Principais tipos de ameaças

Percurso

Etapa 4 Boas práticas em cibersegurança

Etapa 5 Red Team VS Blue Team

Etapa 1

Cibersegurança, o que é?

Introdução

Nesta aula vamos conhecer os conceitos que forma esta área tão vasta.

Definição

*"A cibersegurança é um **conjunto de ações e técnicas** para **proteger sistemas, programas, redes** e **equipamentos** contra **invasões**."*

Definição

Tem foco em garantir que dados valiosos não vazem ou sejam violados em ataques cibernéticos.

Sobre cibersegurança

De acordo com uma pesquisa da Netscout (2022):

- O Brasil é o **2º país do mundo** em que mais ocorrem ciberataques;
- Mais de **439 mil** tentativas de invasões e de ataques de negação de serviço distribuído (DDoS) registrados, atrás apenas dos EUA.

Função da cibersegurança

- Voltada para softwares, hardwares e redes;
- Previne problemas com a gestão de informações;
- Protege os dados armazenados.

Tipos de cibersegurança

Dentro do universo da cibersegurança, algumas categorias podem ser definidas, dependendo do contexto.

Tipos de cibersegurança

- Segurança Operacional
- Segurança de Rede
- Segurança de Aplicativos
- Educação do Usuário Final
- Recuperação de desastres

Segurança operacional

É parte das rotinas de segurança operacional, na qual a empresa protege seus dados definindo quem acessa e os níveis de acesso.

Segurança de rede

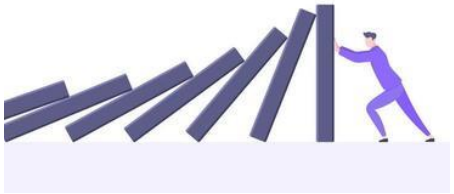
É encarregada de proteger a rede contra acessos indevidos e ataques como DoS (Denial of Service).

Segurança de aplicativos

É a resposta contra as ameaças aos softwares instalados nos computadores e dispositivos móveis em geral, implementando protocolos de segurança durante seu desenvolvimento.

Recuperação de desastres

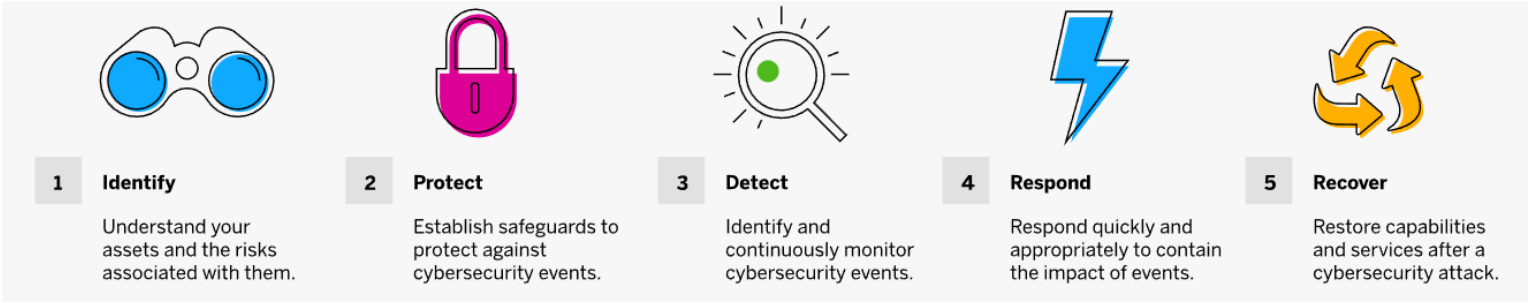
Define as práticas que uma organização utiliza em caso de desastres, para que possa se recuperar da forma mais rápida possível e com o menor dano possível.



Educação do usuário final

Encontrar e corrigir comportamentos de riscos dos usuários que podem expor dados sensíveis ou colocar uma organização em risco.

Pilares da cibersegurança



1 Identify

Understand your assets and the risks associated with them.

2 Protect

Establish safeguards to protect against cybersecurity events.

3 Detect

Identify and continuously monitor cybersecurity events.

4 Respond

Respond quickly and appropriately to contain the impact of events.

5 Recover

Restore capabilities and services after a cybersecurity attack.

Conclusão

Nesta aula foram apresentados alguns conceitos à volta da cibersegurança, agora vamos nos aprofundar nas próximas aulas.

Etapa 2

O que é hacking?

Introdução

Nesta aula vamos explorar o termo **hacking** um termo muitas vezes usado de forma equivocada.

Sobre hacking

De forma geral, o termo *hacking* significa: *"comprometer sistemas de computador, contas pessoais, redes de computador ou dispositivos digitais"*.

Sobre hacking

Porém não significa necessariamente um ato mal-intencionado, pois o termo pode ser utilizado para o uso da tecnologia ou um conhecimento para contornar um desafio.

O que é um hacker?

O hacker é uma pessoa que utiliza seus conhecimentos e tecnologias para driblar mecanismos e acessar ou comprometer informações e sistemas.

Hacker vs Cracker

Quando um hacker invade uma rede ou sistema, violando a segurança, de forma **maliciosa**, estamos falando na verdade de um **cracker**.

Tipos de hackers

Hackers podem ser classificados com base na legalidade do que fazem, sendo **black hat**, **white hat** e **grey hat**.

Hackers black hat

Hackers do tipo **black hat** (chapéu preto) são pessoas que utilizam conhecimento e tecnologia para fins maliciosos como vazamento de dados, comprometimento de sistemas e extorsão.

Hackers white hat

Hackers do tipo **white hat** (chapéu branco), também conhecido como **hacker ético**, utiliza os conhecimentos e tecnologia para detectar ameaças e proteger sistemas, com base em acordos e contratos.

Hackers grey hat

São um tipo intermediário, onde começam testando os sistemas ou softwares de uma empresa para identificar falhas de segurança e depois avisam a organização para oferecer uma solução.

Legalidade

Todo hacking do tipo black hat é ilegal, pois não há consentimento prévio da parte invadida, enquanto o white hat é feito totalmente baseado em acordos e limites estabelecidos entre as partes.

Tecnicas de hacking

- Phishing
- Spoofing de DNS
- Roubo de Cookies
- XSS
- SQL Injection

Conclusão

O termo *hacking* vai muito além de apenas ataques e invasões de sistemas e redes.

Etapa 3

Principais tipos de ameaças

Introdução

Nesta aula vamos conhecer os principais tipos de ameaças contra aplicações e redes de computadores.

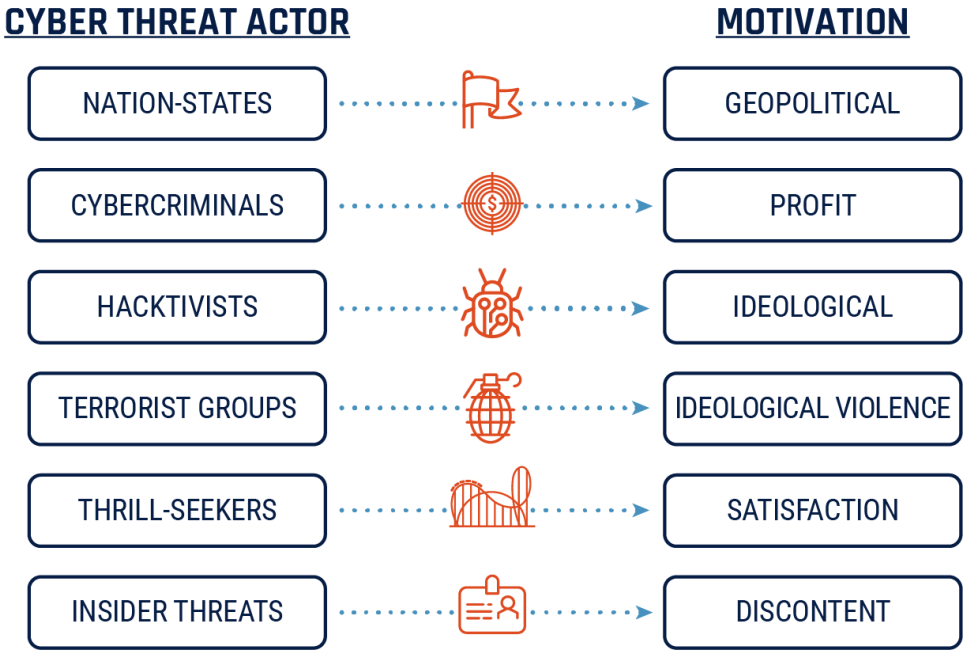
Introdução

As ameaças não são direcionadas apenas contra os sistemas ou às redes de computadores de uma organização, mas também contra as pessoas que fazem parte da mesma.

Fontes de ataques

As ameaças podem surgir de uma variedade de lugares, pessoas e contextos, como as descritas a seguir:

Fontes de ataques



Tipos de ataques

Conclusão

Há um número cada vez mais crescente da quantidade e tipos de ataques cibernéticos, um problema que abre por outro lado um leque enorme para os profissionais.

Etapa 4

Boas práticas em cibersegurança

Introdução

Depois de vermos várias formas e fontes de ameaças, vamos conhecer as boas práticas utilizaas no combate e prevenção de ataques cibernéticos.

Boas práticas

Existem uma série de boas práticas que envolvem desde a utilização de sistemas seguros e confiáveis, até a mudança de comportamentos dos usuários.

Categorias de boas práticas

- Conscientização de pessoas;
- Controle de acesso a ativos críticos;
- Proteção de dados confidenciais;
- Segurança robusta e proteção de rede;
- Gerenciamento de identidades.

Conscientização de pessoas

- Abordagem de segurança centrada nas pessoas;
- Reduzir o nível de negligência dos funcionários;
- Informe os funcionários sobre técnicas comuns de phishing.

Controle de acesso a ativos críticos

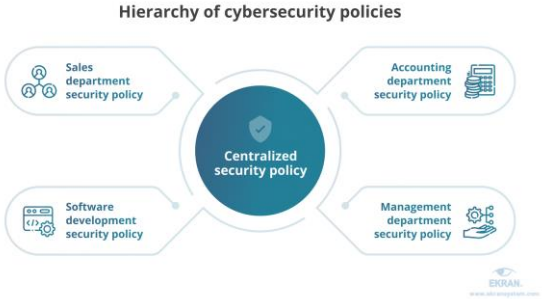
- Proteção o acesso de dispositivos remotos;
- Manipular as senhas com segurança;
- Usar o **princípio do privilégio mínimo**;

Proteção de dados confidenciais

- Atenção nos usuários privilegiados;
- Monitoramento de acesso de terceiros aos dados;
- Manter backup de seus dados confidenciais.

Segurança robusta e proteção de rede

- Uso de políticas hierárquicas de segurança cibernética;
- Proteger a rede corporativa;
- Auditorias regulares de segurança cibernética.



Gerenciamento de identidades

- Empregar segurança biométrica;
- Usar autenticação multifator.

Conclusão

Boas práticas podem fazer a diferença entre a vida e a morte de uma organização, tendo em vista o alto dano financeiro e de reputação causados por ataques cibernéticos.

Etapa 5

Blue Team VS Red Team

Introdução

Devido ao aumento da quantidade e complexidade das ameaças cibernéticas, as organizações tem utilizado uma abordagem mais estratégica na questão da segurança.

Introdução

É nesse contexto que as organizações formam times como o ***Red Team*** e ***Blue Team*** que ensaiam técnicas de ataque e defesa, visando identificar e corrigir possíveis falhas de segurança.

Blue Team e Red Team

Red Team

O Red Team é formado com o objetivo de realizar testes de ciberataque com profissionais de alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de penetrar na rede e ou sistemas.

Blue Team

O papel do Blue Team é se opor aos ataques ensaiados pelo Red Team, desenvolvendo estratégias para aumentar as defesas, modificando e reagrupando os mecanismos de proteção da rede para que eles se tornem mais fortes.

Blue Team, Red Team e Purple Team

Purple Team

Um *Purple Team* é a fusão entre *Blue Team* e *Red Team*, sendo uma combinação de profissionais de segurança cibernética, que atuam como uma única unidade.

Purple Team

Desempenha as funções de ambos os times, mas com vantagens como a melhor comunicação, compartilhamento de conhecimento e melhoria de segurança, além da otimização do tempo.

Certificações

Certified Ethical Hacker (CEH);

EC-Council Certified Security Analyst (ECSA).

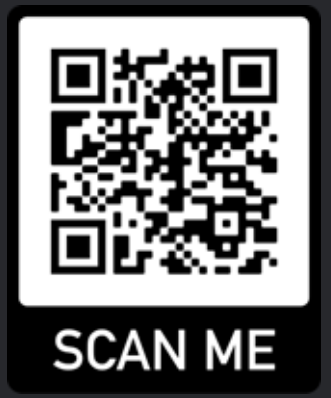
Conclusão

Vimos durante esta aula como as empresas se preparam contra as ameaças cibernéticas, o que demanda alta especialização dos profissionais.

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)



Links Úteis

- **Referências:**
  - **European Union Agency for Cybersecurity**