Prime

CCS - A

Conceitos da Cybersecurity

Conceito de Cybersecurity

CONCEITO:

Cibersegurança, ou Segurança Cibernética, é a prática de proteger sistemas, redes e programas contra ataques digitais.

Tipos de Segurança

Segurança Física;

Segurança de Comunicação;

Segurança do Computador;

Segurança de Rede.

Segurança Física

- A segurança física é o conceito de poder controlar quem tem acesso físico aos ativos dentro da organização.

Exemplos:

- Acesso aos servidores em uma sala trancada;
- Quem pode entrar nas instalações da organização;
- Cercar ao redor do perímetro da instalação;
- Usando guardas no portão de entrada.

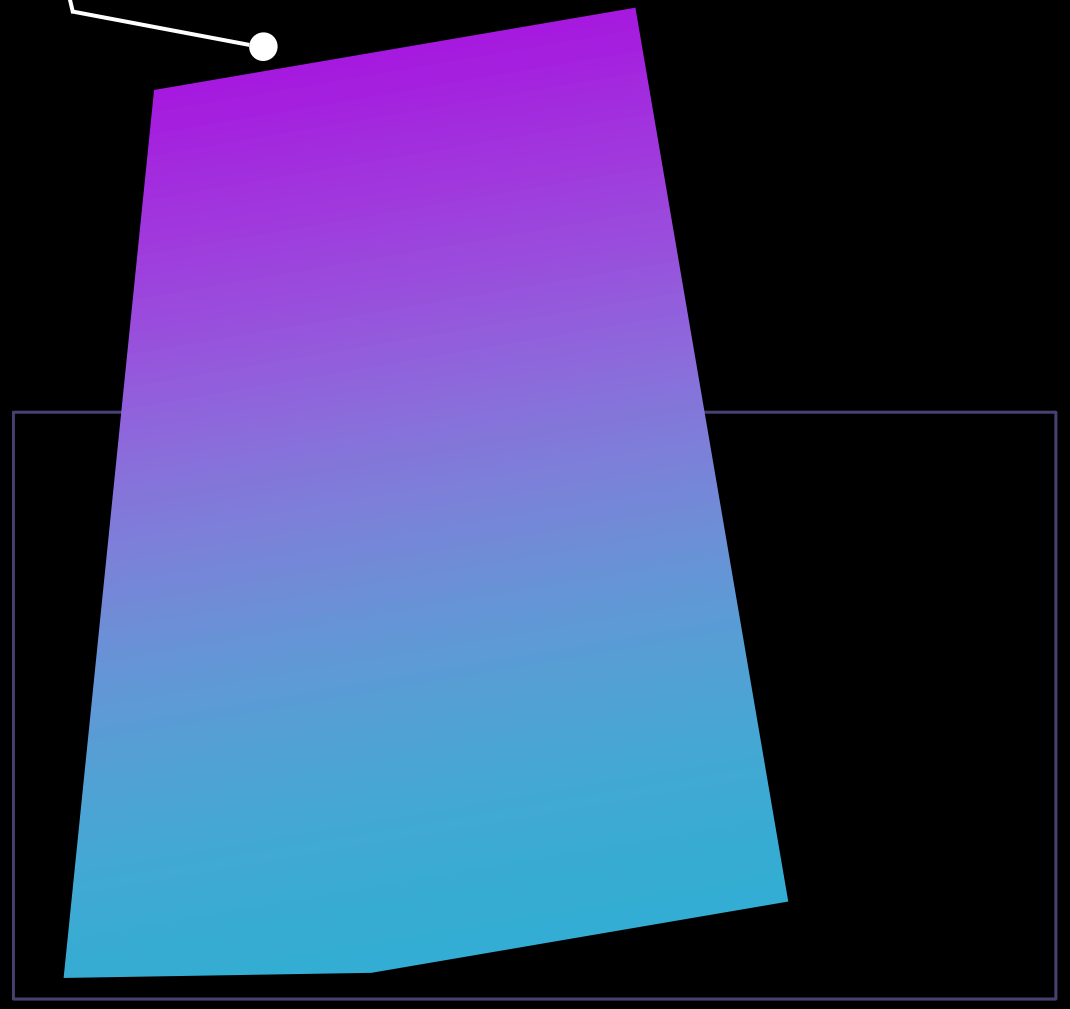
Segurança de Comunicação

- Informações que trafegam entre a origem e o destino, criptografando a comunicação;
- Enquanto um arquivo é baixado para o computador;
- Ao enviar um e-mail.

CONCEITOS DA CYBERSECURITY

Segurança do Computador

- Autenticação no computador e sistemas;
- Controle de acesso ao equipamento;
- Redundância de dados;
- Proteção contra malware;
- Outras técnicas de proteção do sistema.



Segurança de Rede

- Controlar quem obtém acesso à rede;
- Segurança do switch e roteador;
- Tipo de tráfego pode entrar na rede (firewalls);
- Monitoramento do tráfego de rede em busca de atividades suspeitas (um sistema de detecção de intrusão).

Noções Básicas Sobre Princípios de Segurança da Informação

- Privilégio Mínimo;
- Separação de Funções;
- Rotação de Funções;
- Conceito de “Need to Know”;
- Segurança em Camadas;
- Diversidade de Defesa;
- Due Diligence e Due Care;
- Vulnerabilidade e Exploração.

CONCEITOS DA CYBERSECURITY

Privilégio Mínimo

OBJETIVO:

Conceder a um usuário apenas o nível mínimo de permissões necessárias para realizar suas tarefas ou deveres.

EXEMPLOS:

- Para fazer backup em um computador, não há a necessidade de ser admin;
- Se um usuário precisa apenas ler o conteúdo de um arquivo, certifique-se de conceder a ele apenas a permissão de leitura.

CONCEITOS DA CYBERSECURITY

Separação de Funções

OBJETIVO:

Garantir que todas as tarefas críticas sejam divididas em diferentes processos e que cada processo seja executado por um funcionário diferente.

EXEMPLOS:

- A pessoa que preenche o cheque é diferente de quem assina;
- Teste feito por outra pessoa ou equipe;
- Alguém resolve um problema e outro pessoa coloca em produção.

CONCEITOS DA CYBERSECURITY

Rotação de Funções

- Rotação de funções é o princípio de rotação de vários funcionários por diferentes funções de trabalho.

OBJETIVO:

- É uma forma de garantir a responsabilidade pelas ações dos funcionários;
- A organização passa a não depender de uma única pessoa capaz de desempenhar uma função de trabalho.

EXEMPLOS:

- Neste mês João cuidará do gerenciamento de contas, mas no próximo mês Maria assumirá essa função e João assumirá a função que Maria tinha.
- João entrou de férias ou se ausentou e é substituído por Maria;
- Denunciar trabalho, identificar melhorias, redundância etc.

Conceito de “Need to Know”

- Dar aos funcionários acesso apenas às informações que eles precisam saber.

EXEMPLOS:

- Sysadmin precisa ter acesso aos dados do RH?
- Os gerentes devem ter acesso aos dados contábeis ou apenas o gerente de contabilidade?
- A equipe de Call Center precisa ter acesso a todos os dados dos clientes?

Segurança em Camadas

- A segurança em camadas é o conceito de “não colocar todos os ovos em uma única cesta”;
- Conta com um tipo de solução de segurança por camada para criar um ambiente seguro.
- Diferentes controles de segurança, como autenticação, proteção contra vírus, sistemas de patches e firewalls.

Diversidade de Defesa

Diversidade de defesa significa usar produtos diferentes para aumentar o nível de segurança em seu ambiente.

EXEMPLOS:

- Importante não usar o mesmo produto de firewall em cada camada;
- Sistema de antivírus no PC diferente do que tem no servidor.

Diligência Devida e Cuidado Devido

CONCEITOS DA CYBERSECURITY

OBJETIVO:

Garantir que a organização esteja tomando medidas para fazer a coisa certa para proteger seus funcionários e ativos.

É fazer a coisa certa!

- O cuidado devido trata-se das precauções tomadas pelos colaboradores, exemplo: não abrir um e-mail suspeito.
- A diligência devida trata de identificar os riscos e prevenir a ocorrência de problemas, exemplo: avaliações regulares nos controles.

Vulnerabilidade e Exploração

- Uma vulnerabilidade é uma fraqueza em um software ou hardware que foi criada acidentalmente pelo fabricante.

- Uma vez que os hackers encontram uma fraqueza, eles trabalham em uma maneira de explorar a fraqueza e comprometer a segurança do sistema.

OBRIGADO !

CONCEITOS DA CYBERSECURITY