SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE II – IMPLEMENTAÇÃO DA SEGURANÇA NOS DADOS

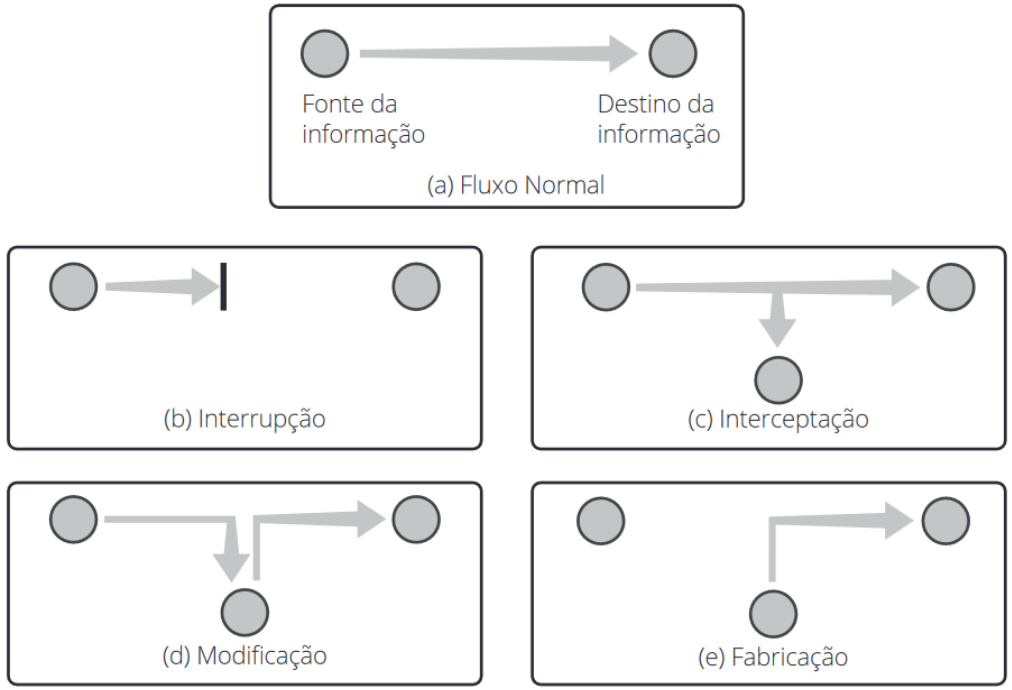
PUC Minas
Virtual

2.1 – TIPOS DE ATAQUE AOS DADOS CORPORATIVOS

PUC Minas
Virtual

2.1.3 – MODELOS DE ATAQUES CIBERNÉTICOS

MODELOS DE ATAQUES CIBERNÉTICOS



Fonte: Coelho, 2013.

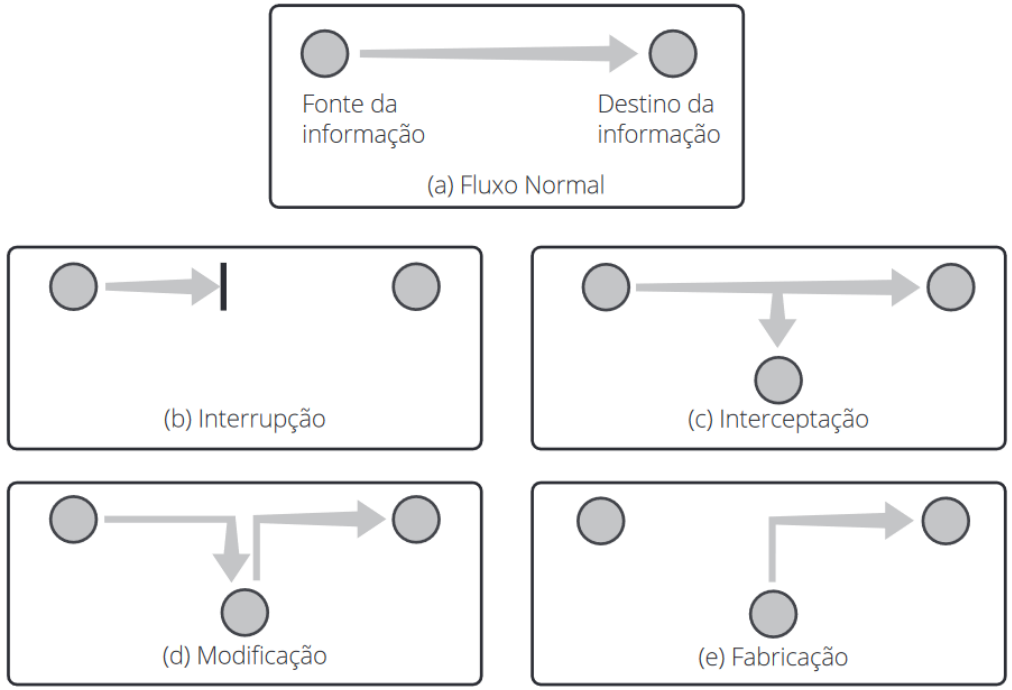
a) INTERRUPÇÃO

Ocorre quando há a destruição ou indisponibilidade de um ativo corporativo caracterizando um ataque contra a disponibilidade. Um exemplo é a destruição de um disco rígido

b) INTERCEPTAÇÃO

Ocorre quando um ativo é acessado por pessoa, programa ou outro equipamento não autorizado, caracterizando um ataque contra a confidencialidade. A cópia não autorizada de arquivos ou programas é um exemplo

MODELOS DE ATAQUES CIBERNÉTICOS



Fonte: Coelho, 2013.

c) MODIFICAÇÃO

Ocorre quando um ativo é acessado por pessoa, programa ou equipamento não autorizado e ainda alterado, caracterizando um ataque contra a integridade. Mudanças em valores em um arquivo de dados são um exemplo

d) FABRICAÇÃO

Percebe-se este ataque quando uma pessoa, programa ou computador não autorizado insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade. A adição de registros em um arquivo são um exemplo deste tipo de ataque.

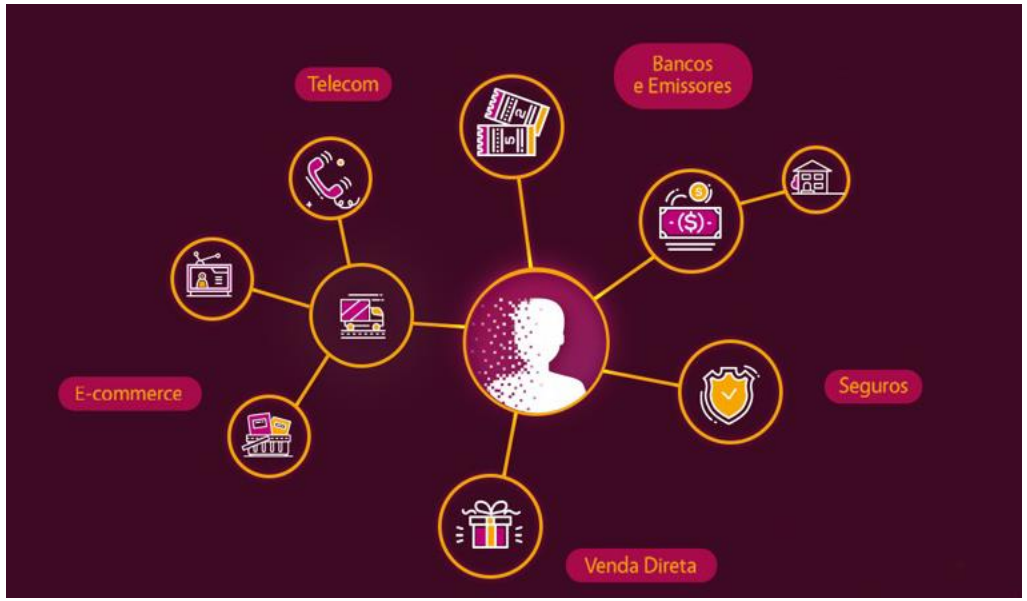
SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

- Assuntos como **criptomoedas**, *Internet of Things* **(IoT)**, *Big Data* & *Analytics*, *Cloud & Data Center* e **Serviços Gerenciados**, além de conectividade de dados e serviços de voz, sequestro de dados, globalização do sinal de rede sem fio (*wi-fi*) e principalmente acesso a dados confidenciais dentro das organizações são atrativos para os invasores.
- Desta forma temos que nos preparar para os tipos de ataques a partir do momento em que disponibilizamos nossas informações em um ambiente público.
- Vamos elencar as principais ameaças para as empresas:

Fonte: Oliveira, 2021.

a) SCAN

Acessar à rede por meio de *backdoors* (brechas implantadas na estrutura da rede) ou de alguma outra forma. Geralmente esta falha está relacionada às versões de firmwares de dispositivos.



Fonte: HANSEN, 2019.

b) FRAUDE

São inúmeras as técnicas para causar este tipo de dano e a mais comum é o PHISHING, onde cria-se um site falso oriundo de um site verdadeiro e o link é enviado por algum mecanismo de mensagem seja ele instantâneo ou não.

Fonte: GUEDES, 2020.

c) WORM

São softwares desenvolvidos com o objetivo de causar algum dano ao computador, smartphone, tablet, etc. possuem funcionalidades infinitas e entre elas monitoramento, espionagem, roubo de informações.

Fonte: SADI, 2018.

d) ENGENHARIA SOCIAL

O foco é o ser humano. Este tipo de ameaça não tem envolvimento direto com o mundo virtual. O objetivo é explorar a ingenuidade, ou a confiança, do usuário para obter informações privilegiadas de acesso a sistemas, dados de cartão de crédito, login e senha, entre outros dados.

VULNERABILIDADES MAIS COMUNS NOS AMBIENTES CORPORATIVOS

ARMAZENAMENTO

- É comum os métodos de armazenamento apresentarem falhas, deixando pessoas não autorizadas terem acesso a alguns conteúdos. Oferece-se visualizar comportamentos inadequados ou irregulares por meio de sistemas de controle de arquivos

COMUNICAÇÃO

- A transmissão de informações corporativas sempre foi alvo de programas e pessoas mal-intencionadas seja por e-mails ou mensagens instantâneas.

VULNERABILIDADES MAIS COMUNS NOS AMBIENTES CORPORATIVOS

INFRAESTRUTURA

- Prática normal recomendada pela segurança da informação é que a infraestrutura de TI esteja atualizada. Recomenda-se que nem sempre a utilização das versões mais atualizadas de hardware e software sejam implantadas antes de conhecer suas possíveis vulnerabilidades.

PESSOAS

- As pessoas lidam de formas diferentes com alguns acontecimentos do dia e o excesso de confiança grande parte das vezes gera uma situação frágil em alguns sistemas.

REFERENCIAS BIBLIOGRÁFICAS

CORREA JUNIOR, H. E. Segurança de sistemas: conceitos básicos: material adaptado da Academia Latino-Americana de Segurança - Microsoft. 2011. Disponível em: <https://pt.scribd.com/document/84971695/aula1>. Acesso em: 20 ago. 2022.

DANTAS, L. M. Segurança da informação: uma abordagem focada em gestão de riscos. Olinda, PE: Livro Rápido, 2011.

OLIVEIRA, Marcos. Segurança da Informação – Conscientização. Disponível em: https://terminalroot.com.br/2021/02/os-6-melhores-scanners-de-rede-para-linux.html>. Acesso em 10 Ago. 2022.

THOMAS Erl, RICARDO Puttini, ZAIGHAM Mahmood. Cloud Computing: Concepts, Technology & Architecture. Pearson. Oreilly 2013.

REFERENCIAS BIBLIOGRÁFICAS

Sadi, 2018. Por que sua empresa deve ser preocupar com a Engenharia Social? Proteja a segurança de TI. Disponível em:< https://www.scurra.com.br/blog/por-que-sua-empresa-deve-ser-preocupar-com-a-engenharia-social-proteja-a-seguranca-de-ti/ >. Acesso em: 30 ago. 2022.

GUEDES, Kayobrussy 2020. Vírus vs. Worm: Qual é a diferença?. Disponível em:<https://www.topgadget.com.br/howto/seguranca-howto/virus-vs-worm-qual-e-a-diferenca.htm>. Acesso em: 6 Set. 2022.

HANSEN, Gilmar. Antifraude: como o efeito de rede protege nossos clientes. Disponível em: <https://blogbr.clear.sale/antifraude-como-o-efeito-de-rede-protege-nossos-clientes>. Acesso em: 14 Set. 2022.


PUC Minas
Virtual