SEGURANÇA E DIREITO DIGITAL
UNIDADE 1: SÍNTESE

Gabriel Mitelman Tkacz
42230446@mackenzista.com.br
Universidade Presbiteriana Mackenzie, Faculdade de Computação e Informática
São Paulo, fevereiro de 2023

1. *As medidas de segurança adotadas são capazes de proteger completamente contra ataques?*

    Embora seja importante adotar medidas de segurança e aplicar políticas preventivas, não é possível garantir que um sistema seja completamente imune a ataques. Isso ocorre porque sempre há novas vulnerabilidades e formas de ataque que ainda não foram identificadas e prevenidas. Além disso, muitas vezes os próprios usuários podem inadvertidamente introduzir brechas de segurança, como por exemplo, clicar em um link malicioso ou compartilhar informações confidenciais sem o devido cuidado. Por isso, é importante adotar uma abordagem de segurança em camadas, que combine diversas medidas de segurança em diferentes níveis, como por exemplo, firewall, antivírus, criptografia e autenticação, para reduzir o risco de ataques bem-sucedidos.

2. *O comportamento humano influencia uma possível falha na segurança de sistemas computacionais seguros?*

    Sim, o comportamento humano pode influenciar significativamente a segurança dos sistemas computacionais. Isso ocorre porque muitas vezes são as ações dos usuários que possibilitam que as vulnerabilidades sejam exploradas pelos atacantes. Por exemplo, um usuário pode utilizar senhas fracas ou compartilhá-las com terceiros, clicar em links maliciosos em e-mails ou em redes sociais, ou ainda instalar softwares não confiáveis ou não atualizados. Além disso, a falta de conscientização e treinamento dos usuários pode levar a erros de configuração ou outras vulnerabilidades de segurança através da engenharia social. Por isso, é importante conscientizar os usuários sobre boas práticas de segurança e fornecer

treinamentos regulares para evitar que esses comportamentos sejam repetidos e para que possam adotar medidas preventivas em seus hábitos de navegação.

3. *Falta de senhas de acesso, falta de instalação de detectores de malwares, configuração incorreta de data e hora no computador, entre outras atitudes, são consideradas falhas do usuário ou da política de segurança?*

A falta de senhas de acesso, falta de instalação de detectores de malwares, configuração incorreta de data e hora no computador, entre outras atitudes, podem ser consideradas falhas tanto do usuário quanto da política de segurança. É responsabilidade do usuário seguir as orientações de segurança e adotar medidas preventivas, como definir senhas fortes, manter o software atualizado e configurar corretamente o sistema. No entanto, também é dever da política de segurança estabelecer normas claras e oferecer suporte para garantir que as medidas de segurança sejam de fato aplicadas. Isso inclui fornecer treinamentos regulares sobre boas práticas de segurança, definir políticas claras sobre uso de software e equipamentos, bem como monitorar a segurança dos sistemas para identificar possíveis vulnerabilidades e tomar as medidas necessárias para corrigi-las.