Aplicações dos conteúdos estudados em SCS

Os conteúdos trabalhados na disciplina de **Sistemas Computacionais e Segurança (SCS)** possuem aplicações diretas e muito relevantes no cotidiano da área de Tecnologia da Informação e Comunicação. Um primeiro exemplo está na **segurança de dispositivos móveis**, como smartphones e tablets, que hoje concentram boa parte das informações pessoais e profissionais. Medidas como a autenticação biométrica (uso de impressão digital ou reconhecimento facial para liberar o acesso), o uso de senhas fortes e a instalação de aplicativos somente de fontes confiáveis são práticas que reduzem significativamente a possibilidade de ataques e roubo de dados sensíveis.

Outro ponto de aplicação fundamental é o **controle de acessos em empresas**. Essa prática define quem pode acessar determinados arquivos, sistemas ou áreas da rede corporativa. Uma política bastante utilizada é a do *menor privilégio* (cada usuário só tem acesso ao que realmente precisa para realizar suas tarefas). Aliada à autenticação multifator (uso de dois ou mais métodos de verificação, como senha e código enviado por SMS), essa medida impede que invasores explorem credenciais roubadas para obter acesso a dados críticos da organização.

Também merece destaque a aplicação em **auditoria e monitoramento de logs**. Logs são registros automáticos que os sistemas mantêm de todas as suas atividades, como tentativas de login, acessos a arquivos ou execução de programas. Quando analisados de forma estratégica, esses registros permitem identificar comportamentos suspeitos, como múltiplas falhas de login em sequência ***(possível tentativa de ataque por força bruta)*** ou acessos fora do horário normal de trabalho. Esse monitoramento contínuo possibilita que incidentes sejam detectados rapidamente e tratados antes que causem grandes prejuízos.

Outro campo de grande impacto é a **segurança em comércio eletrônico**. Sites de compras online precisam aplicar técnicas como criptografia (processo de transformar informações em códigos indecifráveis para proteger dados durante a

transmissão), o uso de certificados digitais (tecnologia que garante a identidade de um site legítimo, visível no navegador pelo cadeado ao lado do endereço "https://") e sistemas antifraude que analisam transações suspeitas em tempo real. Essas medidas aumentam a confiança dos consumidores, ao mesmo tempo em que protegem informações sensíveis, como senhas e números de cartões de crédito.

Por fim, outra aplicação bastante prática encontra-se nas **políticas de uso de redes Wi-Fi**. Muitas vezes subestimadas, as redes sem fio podem ser portas de entrada para invasores se não forem configuradas corretamente. O uso de criptografia WPA3 (o padrão mais recente para proteger redes Wi-Fi) e a segmentação de redes (separar, por exemplo, a rede de visitantes da rede principal da empresa) são estratégias que reforçam a segurança e evitam que dispositivos não autorizados comprometam a comunicação. Além disso, senhas simples ou compartilhadas entre muitas pessoas devem ser evitadas, uma vez que facilitam ataques de intrusos.

Tópicos Abordados – Aplicações de SCS

- **Segurança em Dispositivos Móveis**
- **Controle de Acessos em Empresas**
- **Auditoria e Monitoramento de Logs**
- **Segurança em Comércio Eletrônico**
- **Políticas de Uso de Redes Wi-Fi**

Nome: Gustavo Jaccon Franquini

RA: 825150548