1.Confidencialidade

A confidencialidade impede a divulgação de informações para pessoas, recursos ou processos não autorizados e garante que as informações apenas sejam acessíveis por pessoas autorizadas, isso significa que os dados não devem ser expostos a pessoas não autorizadas. Empresas restringem o acesso para garantir que apenas os operadores autorizados possam usar os dados ou outros recursos de rede. Os métodos para garantir confidencialidade incluem a criptografia, autenticação e o controle de acesso aos dados.

Há três tipos de informações confidenciais:

- Informações pessoais (identificação)
- Informações comerciais
- Informações confidenciais (órgão/governo)

A maioria dos dados de privacidade são confidenciais, mas nem todos os dados confidenciais são privados. O acesso à informação ocorre após a confirmação de autorização adequada. Criminosos virtuais podem capturar, salvar e roubar dados em trânsito. Profissionais de segurança cibernética devem tomar medidas para combater essas ações.

Ao habilitar a criptografia, os dados legíveis são chamados de texto simples ou texto claro, enquanto a versão criptografada é chamada de texto criptografado ou texto cifrado. Neste curso, usaremos o termo ciphertext. A mensagem legível em texto simples é convertida em texto cifrado, que é a mensagem disfarçada ilegível. A descriptografia reverte o processo. Uma chave é necessária para criptografar e descriptografar uma mensagem. A chave é a ligação entre o texto simples e o cipproxto.

2.Integridade

A integridade se refere à precisão, consistência e a confiabilidade dos dados durante seu ciclo de vida e garante que as informações permaneçam precisas, completas e íntegras, protegendo-as contra alterações não autorizadas. Os dados passam por várias operações, como captura, armazenamento, recuperação, atualização e transferência. Eles devem permanecer inalterados durante todas essas operações por entidades não autorizadas. Os métodos usados para garantir a integridade de dados incluem hashing, verificações de validação de dados, verificação de consistência dos dados e controle de acesso.

Sua necessidade varia com base na organização usando estes dados. A perda da integridade de dados pode tornar recursos de dados inteiros não confiáveis ou inutilizáveis.

- **Baixo nível:** Blogs e sites de postagens pessoais. Os dados podem não ser verificados e ter um baixo nível de confiança no conteúdo.
- **Nível intermediário:** Vendas on-line e mecanismos de busca ocorrendo pouca verificação. Os dados não são totalmente confiáveis.
- **Nível alto:** Comércio eletrônico e análise, onde todos os dados são válidos e conferidos para garantir a confiabilidade.

- **Nível crítico:** Serviços de saúde e emergência. Todos os dados são válidos e testados para garantir a confiabilidade.

Criminosos virtuais podem interceptar e modificar dados em trânsito. Os profissionais de segurança cibernética implantam sistemas de integridade de dados que testam a integridade e a autenticação dos dados transmitidos para combater essas ações.

3.Disponibilidade

A disponibilidade garante que as informações estejam acessíveis para usuários autorizados quando necessário e garante que as informações estejam disponíveis quando necessário Isso implica que sistemas e dados devem estar acessíveis e funcionais, sem interrupções não planejadas. Ataques cibernéticos e falhas do sistema podem impedir o acesso a sistemas e serviços de informação. Os métodos para garantir a disponibilidade incluem a redundância, backups, maior resiliência, manutenção de equipamentos, sistemas operacionais e softwares do sistema, todos atualizados e planos para recuperação rápida de desastres não previstos.

O termo **alta disponibilidade** descreve sistemas concebidos para evitar períodos de inatividade. A alta disponibilidade garante um nível de desempenho por um período maior que o período normal. O objetivo é a capacidade de continuar a operar em condições extremas, como durante um ataque. **Os cinco noves** se referem a 99,9999%, isso significa que o período de inatividade é menos que 5,26 minutos por ano.

Sistemas de alta disponibilidade são projetados incluindo 3 princípios:

- Eliminar pontos únicos de falha
- Proporcionar transição confiável com sistemas de energia
- Detectar falhas à medida em que ocorrem através do monitoramento.

Três abordagens para garantir os cinco noves são ***sistemas padronizados***, ***sistemas de comportamento compartilhado*** e ***clustering***.

Geralmente, empresas garantem a disponibilidade implementado a manutenção de equipamentos, atualizações do SO, sistemas de backup, planos para desastres, implementações tecnológicas e o teste e monitoramento de sistemas.

Criminosos virtuais podem usar dispositivos falsos ou não autorizados para interromper a disponibilidade dos dados. Um simples dispositivo móvel pode servir como um ponto de acesso sem fio local e enganar usuários desavisados para se associarem a um dispositivo falso. Os criminosos virtuais podem sequestrar uma conexão autorizada a um serviço ou dispositivo protegido. Os profissionais de segurança de rede podem implementar sistemas de autenticação mútua para combater essas ações. Os sistemas de autenticação mútua exigem que o usuário se autentique no servidor e solicitem que o servidor se autentique no usuário. Contramedidas são VPNs, SSL, IPsec, criptografia, hashing, redundância e host standby.