Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

CRIPTOGRAFIA

Edição nº15
Setembro/2021

É a arte ou ciência de escrever uma informação em forma cifrada ou em código, usada para diversos fins, utilizando um conjunto de técnicas que torna a mensagem incompreensível. Essa mensagem é comumente chamada de "texto cifrado", permitindo que apenas o destinatário desejado consiga decodificar e ler o texto enviado com clareza, também chamado de "texto plano" ou "texto limpo".

A criptografia fornece técnicas para codificar e decodificar dados, tais que os mesmos possam ser armazenados, transmitidos e recuperados sem sua alteração ou exposição. Em outras palavras, as técnicas de criptografia podem ser usadas como um meio efetivo de proteção de informações suscetíveis a ataques, estejam elas armazenadas em um computador ou sendo transmitidas pela rede.

O processo criptográfico consiste em transformar um texto simples, através de uma função parametrizada por uma chave (senha), em um texto inteligível.
Após o processo de criptografia, o texto poderá ser transmitido ao destinatário.

O destinatário conhece o método utilizado para a criptografia e também conhece a chave, possibilitando a transformação do texto criptografado em texto simples novamente.

Se a mensagem for interceptada por alguém, será necessário descobrir a chave de criptografia bem como o seu método para que se possa ler a mensagem capturada.

Os principais métodos de criptografia são:

- **Criptografia simétrica: utiliza uma chave única para cifrar e decifrar a mensagem e, nesse caso a chave deve ser compartilhada entre o emissor e o receptor da mensagem.**
- **Criptografia assimétrica: utiliza um par de chaves (uma de conhecimento público e outra privada), sendo uma chave para cifrar a informação e uma outra chave diferente para decifrar a informação, onde o que for encriptado utilizando uma chave, só poderá ser lido com o uso da outra.**
- **Criptografia quântica: utiliza algumas características fundamentais da física quântica as quais asseguram o sigilo das informações.**

A criptografia computacional é utilizada para garantir:

- **Confidencialidade: somente os usuários autorizados tem acesso à informação;**
- **Integridade: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente e nem acidentalmente;**
- **Autenticação do remetente: é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente;**
- **Autenticação do destinatário: consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.**

A criptografia é um elemento fundamental da segurança de dados mas, infelizmente, não irá solucionar todos os problemas de segurança.

Existem algumas situações onde, por melhor que sejam os processos de criptografia, não é possível a proteção dos dados, tais como:

- **Ela não impede um atacante de apagar todos os dados;**
- **Um atacante pode comprometer o programa de criptografia modificando o programa para usar uma chave diferente ou gravar as chaves para uma análise posterior;**
- **Um atacante pode encontrar uma forma de decriptografar a mensagem dependendo do tipo de algoritmo utilizado;**
- **Um atacante pode se utilizar de técnicas de Engenharia Social e enganar o usuário, ao se passar por alguém de confiança para que o usuário lhe forneça sua chave.**

Por tudo isso, a criptografia deve fazer parte da estratégia de segurança, combinado com outros métodos que garantam a segurança do processo como um todo.

Fique ligado: no próximo mês, falaremos sobre *Engenharia Social*!

Tribunal Regional Eleitoral - RN