1.Controles criptográficos

Cada pessoa envolvida com TI e segurança de TI deve ter um entendimento básico dos conceitos “criptografia”, “assinatura digital” e “certificados”, embora não necessariamente o conhecimento técnico sobre como eles funcionam. De fato, a criptografia foi usada pelos romanos para transmitir mensagens militares. Mesmo que a mensagem caísse nas mãos inimigas, eles não seriam capazes de obter qualquer informação a partir dela, uma vez que a mensagem parecia sem sentido

A pesquisa de algoritmos criptográficos também é referida como criptoanálise e é usada não só para desenvolver algoritmos, mas também para quebrar algoritmos inimigos

A principal razão para usar criptografia é frequentemente vista como um meio de manter a informação confidencial. É importante notar que existem diferentes sistemas de criptografia. Dependendo da capacidade do sistema criptográfico, ele também pode ser usado para outros propósitos. Outros exemplos de onde a criptografia é usada inclui integridade de dados, autenticidade de dados, mecanismos de autenticação e não repúdio à informação.

O objetivo do não repúdio é obter uma prova da ocorrência ou não de um evento ou ação. É importante notar que, embora a tecnologia seja essencial para tornar isso possível, a força de uma aplicação criptográfica reside também nos aspectos organizacionais, tais como a gestão de chaves.

1.1 Políticas de criptografia

Assim como já explicado, criptografia é uma medida que uma organização pode empregar se, por exemplo, dados confidenciais estiverem envolvidos. O uso da criptografia deve ser cuidadosamente considerado e definido em um documento de políticas. Esse documento de políticas é a base para determinar como aplicar a criptografia dentro dos sistemas de informação da organização.

O documento deve conter ao menos as seguintes informações:

- Para que a organização use criptografia. Um aspecto particular a considerar antes de usar a criptografia são as limitações legais na troca de informações cifras com organizações ou departamentos em outros países. Isso é importante, visto que em alguns casos não é permitido usar certos tipos de criptografia ou transportar softwares criptográficos através das fronteiras de países.
- Que tipos de criptografia a organização usa, e em quais aplicações. Isso é importante para limitar qualquer problema proveniente de aplicações ou algoritmos criptográficos incompatíveis. Ao ter uma política corporativa e ao controlar a sua implementação, essas problemas de compatibilidade podem ser reduzidos ao mínimo
- Controle e gerência de chaves. A base de todo sistema criptográfico são as chaves

- Normalmente, os algoritmos de um sistema criptográfico são públicos: a força do sistema está baseada na força das chaves e na habilidade da organização evitar que essas chaves caiam em mãos erradas. É, portanto, primordial para uma organização possuir informações claras e rigorosas sobre como gerenciar essas chaves.
- Ao fazer backup de dados cifrados, é importante determinar como os dados originais podem ser acessados quando requerido. Isso é especialmente importante quando a chave é perdida ou comprometida, o que significa que usuários não autorizados obtiveram acesso à chave.
- O controle descreve a forma como a aplicação de um material criptográfico é tratada pela organização e quais medidas estão em vigor para limitar o uso indevido. Tal uso indevido pode incluir funcionários deliberadamente criptografando dados, sem autorização, deixando a empresa sem acesso às informações.

1.2 Gerenciamento de chaves

O gerenciamento de chaves é uma parte importante de qualquer sistema criptográfico. Chaves criptográficas devem ser protegidas contra alterações, perda ou destruição, uma vez que qualquer uma dessas ações pode resultar na impossibilidade de acessar os dados. Não que os dados sejam realmente perdidos, mas sem a chave apropriada o dado não está disponível em uma forma legível. Um bom gerenciamento de chaves é essencial para manter a confidencialidade dos dados. Como a perda da chave criptográfica é comparável à perda do dado, o gerenciamento de chaves também é importante para a disponibilidade do dado. Adicionalmente, dependendo do uso da criptografia em uma organização, a divulgação não autorizada chave pode ter implicações severas na integridade do dado.

Além disso, quando a criptografia é usada para a confidencialidade dos dados, chaves secretas e pessoais devem ser protegidas contra divulgações não autorizadas, uma vez que isso é potencialmente uma brecha na confidencialidade da informação. Como as chaves são base para qualquer sistema criptográfico, o equipamento que é utilizado para gerar, armazenar e arquivar chaves deve ser protegido fisicamente. Uma parte do gerenciamento de chaves é o registro dos pares de chaves usados para determinar a autenticidade e o não repúdio da mensagem, então o registro deve abranger quais pares foram emitidos para quem e quando. Outros tópicos que devem ser tratados no gerenciamento de chaves incluem por quanto tempo as chaves ficarão válidas e o que deve ser feito se as chaves forem comprometidas.

Ao usar criptografia para proteger a informação armazenada no equipamento, é um alto risco usar as mesmas chaves para todos os equipamentos, ou uma grande parte deles, dentro de uma organização. Se alguma dessas chaves se tornar conhecida fora da organização, então o equipamento terá que receber novas chaves, uma vez que, potencialmente, todos os dados armazenados neste dispositivo ficaram comprometidos

pelo vazamento da chave. Isso pode ser uma operação muito cara, que deve ser realizada bem rapidamente a fim de prevenir uma brecha na confidencialidade da informação. É fácil ver que a força de um sistema criptografado está diretamente relacionada à qualidade do gerenciamento de chaves.

2.Tipos de sistemas criptográficos

Para que sejam capazes de fazer uso de um sistema criptográfico, tanto o remetente quanto o destinatário devem utilizar o mesmo sistema criptográfico. Uma característica de um bom sistema criptográfico é que o algoritmo propriamente dito é público. Em termos gerais, há três formas de algoritmos criptográficos: simétricos, assimétricos e unidirecionais.

2.1 Sistema simétrico

Uma característica de tal sistema é que há um algoritmo e uma chave secreta que o remetente e o destinatário compartilham. Em um sistema de criptografia simétrica é primordial que a chave seja protegida. A mesma chave é usada tanto pelo destinatário quanto pelo remetente. Portanto, a chave secreta deve ser trocada antes da comunicação do transmissor para o receptor, ou se a chave for interceptada por um atacante quando for enviada entre as partes que se comunicam. O risco da chave ser comprometida fica maior com o aumento do número de partes envolvidas na troca de mensagens com a mesma chave.

2.2 Sistema assimétrico

Um sistema assimétrico soluciona a vulnerabilidade envolvida no compartilhamento de chaves secretas. A característica de um sistema assimétrico é que chaves diferentes são usadas para cifrar e decifrar. O aspecto mais impactante desse algoritmo é não ser mais necessário que o transmissor e o receptor tenham a mesma chave. A chave funciona com os chamados pares de chaves. Utilizando esse método, a chave pública é responsável pela criptografia e apenas a chave privada desse par consegue decifrar a mensagem. O que torna esse sistema tão especial é que a chave pública pode ser conhecida pelo mundo inteiro, contanto que a chave privada seja mantida secreta. Sendo assim, esse sistema também é conhecido como criptografia de chave pública.

O sistema assimétrico pode ser utilizado de duas formas. A primeira forma é assinar uma mensagem com uma chave privada. Utilizando a chave pública, o receptor pode verificar se a mensagem foi originada pelo proprietário da chave privada correspondente. A segunda forma é criptografar mensagens destinadas a uma pessoa que tenha sua própria chave pública. Apenas o detentor da chave privada associada a essa chave pública será capaz de decifrar a mensagem.

Tenha em mente que a chave privada só é conhecida pelo proprietário da chave; e como essa chave não precisa ser compartilhada com mais ninguém para se comunicar, ela não é vulnerável a ataques relacionados à troca de chaves, tal como requerido em um sistema simétrico. Uma assinatura digital geralmente consiste de dois

algoritmos: um para confirmar que a informação não foi alterada por terceiros e, portanto, assegurar a integridade da mensagem. O outro algoritmo é para confirmar a identidade da pessoa que “assinou” a informação, portanto, assegurando o não repúdio.

2.3 Infraestrutura de chave pública (PKI)

É baseada em criptografia de chave pública e inclui muito mais do que somente a criptografia. Uma característica de uma PKI é que, através de acordos, procedimentos e uma estrutura organizacional, ela provê garantias referentes a quais pessoas ou sistemas pertencem a uma chave pública específica. Uma infraestrutura de chave pública é frequentemente gerenciada por uma autoridade independente e confiável.

A força de uma PKI depende, em grande medida, de aspectos não técnicos. A forma como o usuário obtém sua chave privada, por exemplo, é uma pedra angular na confiança que outras pessoas têm na solução de PKI, mesmo se tecnicamente elas usarem os mesmos algoritmos e tamanhos de chave. Uma PKI em que os usuários podem obter uma chave privada solicitando-a por e-mail, usando, por exemplo, o gmail, é inerentemente menos confiável para identificar uma pessoa com base em sua chave pública do que um sistema onde usuários têm de se reportar a uma mesa e de identificar, por meio de um passaporte, antes de receber uma chave privada.

Não repúdio é a garantia de que alguém não pode negar algo. Tipicamente, o não repúdio se refere à habilidade em assegurar que uma parte de um contrato, ou de uma comunicação, não pode negar a autenticidade de sua assinatura em um documento ou o envio de uma mensagem que originou. Repudiar significa negar.

Na Internet, uma assinatura digital é utilizada não só para assegurar que um documento tenha sido assinado eletronicamente pela pessoa que supostamente assinou o documento, mas também para garantir que uma pessoa não possa negar mais tarde que forneceu a assinatura, visto que uma assinatura digital só pode ser criada por uma pessoa. Uma PKI é uma solução para alcançar o não repúdio.

A ISO define o não repúdio como a habilidade de provar a ocorrência de um evento ou uma ação reivindicada e suas entidades originárias, a fim de solucionar disputas sobre a ocorrência ou não do evento ou ação e o envolvimento de entidades no evento.

2.4 Sistema unidirecional

Essa forma de criptografia também é chamada de função hash. Uma função hash é um cálculo irreversível. A operação de funções hash pode ser comparada a misturar tintas. Assim que duas cores de tinta se misturam uma com a outra, é impossível separá-las. Por causa dessa característica, esse tipo de algoritmo é utilizado principalmente para determinar se um dado foi alterado.

A mensagem é convertida em um valor numérico chamado de valor de hash. Utilizando um algoritmo conhecido, o destinatário pode verificar se a mensagem tem o valor de hash correto; se dois valores de hash coincidem, a mensagem deve estar

inalterada. hashes também podem ser usados para confirmar se duas mensagens são as mesmas.

Quando uma senha é definida, o sistema cria um hash e então armazena esse valor de hash e não a senha propriamente dita. Dessa forma, mesmo uma pessoa com acesso de alto nível ao sistema não pode ver o que outra pessoa usou como senha. Mais tarde, quando a pessoa apresentar a senha para autenticação, o sistema criará novamente um hash da senha e o compara com o hash armazenado no sistema. Se os hashes coincidirem, a pessoa inseriu a senha correta. É importante compreender que esse método é utilizado para verificar a integridade das mensagens. Ele não provê confidencialidade.