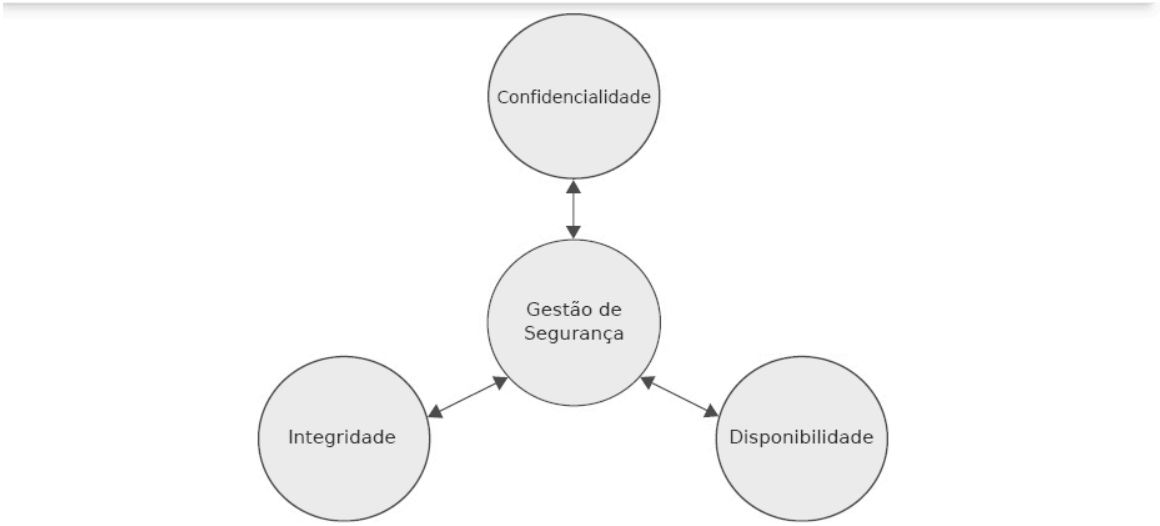
1.Princípios fundamentais da Segurança da Informação

Um programa de segurança pode ter diversos objetivos, grandes e pequenos, mas os princípios mais importantes em todos os programas de segurança são a confidencialidade, integridade e disponibilidade. Estes são referidos como o triângulo CIA.

O nível de segurança requerido para executar esses princípios é diferente para cada empresa, pois cada uma tem sua própria combinação de objetivos e requisitos de negócio e de segurança. Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidas pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CIA.



Confidencialidade, integridade e disponibilidade são os princípios críticos de segurança. Você deve compreender o seu significado, como eles são providos por diferentes mecanismos e como a sua ausência pode afetar negativamente um ambiente. Tudo isso o ajuda a identificar melhor os problemas e a fornecer soluções adequadas.

2.Confidencialidade

A confidencialidade, também chamada de exclusividade, se refere aos limites em termos de quem pode obter que tipo de informação. A confidencialidade assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. Esse nível de confidencialidade deve prevalecer enquanto os dados residirem em sistemas e dispositivos na rede, quando forem transmitidos e quando chegarem ao seu destino.

A confidencialidade pode ser fornecida através da criptografia de dados à medida que são armazenados e transmitidos, usando preenchimento de tráfego na rede, estrito controle de acesso, classificação dos dados e treinamento de pessoal nos procedimentos apropriados.

Exemplos:

01. O acesso à informação é concedido com base na necessidade de conhecer. Não é necessário que um funcionário do departamento financeiro seja capaz de ver relatórios de discussões com clientes.

02. Os funcionários tomam medidas para garantir que a informação não vá para pessoas que não necessitam dela. Eles asseguram que nenhum documento confidencial seja deixado sobre suas mesas enquanto estão ausentes

03. O gerenciamento de acesso lógico assegura que pessoas ou processos não autorizados não tenham acesso a sistemas automatizados, base de dados e programas. Um usuário não tem direito de alterar configurações do PC.

04. É criado uma separação de funções entre a organização de desenvolvimento do sistema, a organização de processamento e a organização do usuário. O desenvolvedor não pode fazer qualquer modificação nos salários.

05. São criadas separações estritas entre o ambiente de desenvolvimento, o ambiente de teste e aceitação, e o ambiente de produção.

No processamento e uso dos dados, são tomadas medidas para garantir a privacidade do pessoal e de terceiros. O departamento de Recursos Humanos pode ter sua própria unidade de rede que não é acessível a outros departamentos.

O uso de computadores por usuários finais é cercado de medidas, de forma que a confidencialidade da informação seja garantida.

As camadas de rede são criptografadas, reduzindo a oportunidade de análise do tráfego. Ainda é possível, nessas condições, um atacante acessar o volume de tráfego na rede e observar o que entra e o que sai de cada sistema final. Uma contramedida para esse tipo de ataque é o “traffic padding”.

O preenchimento de tráfego produz continuamente texto cifrado, mesmo na ausência de texto simples. Um fluxo contínuo de dados aleatórios é gerado. Quando um texto simples está disponível, ele é criptografado e transmitido. Quando não há um texto simples na entrada, dados aleatórios são criptografados e transmitidos. Isso torna impossível para um atacante distinguir entre um fluxo de dados verdadeiro e um preenchimento de dados, e, portanto, reduzir o volume de tráfego.

O preenchimento de tráfego é essencialmente uma função de criptografia de enlace. Se apenas a criptografia fim-a-fim for empregada, então as medidas disponíveis para o defensor são mais limitadas. Se a criptografia for empregada na camada de aplicação, então o oponente pode determinar a camada de transporte, o endereço da camada de rede e os padrões de tráfego, os quais permanecerão todos acessíveis.

3.Integridade

A integridade se refere a ser correto e consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada de dados, deliberada ou acidental, é uma violação da integridade dos dados, por exemplo, é esperado que dados armazenados em disco sejam estáveis.

Para Donn Parker “minha definição para integridade da informação vem dos dicionários. Integridade significa que a informação é completa, perfeita e intacta. Significa que nada está faltando na informação, ela está completa e em um desejado bom estado”.

Ambientes que reforçam e fornecem esse atributo de segurança asseguram que atacantes, ou erros de usuários, não comprometam a integridade dos sistemas ou dados. Quando um atacante insere um vírus, uma bomba lógica ou um backdoor em um sistema, a integridade do sistema é comprometida. Isso pode afetar negativamente a integridade da informação contida no sistema através de corrupção, modificação maliciosa ou substituição de dados por dados incorretos. Controle de acesso restrito, detecção de intrusão e hashing podem combater essas ameaças.

Os usuários normalmente afetam o sistema ou a integridade de seus dados por erro. Modificar incorretamente dados mantidos em banco de dados é outra forma comum dos usuários corromperem acidentalmente os dados, um erro que pode ter efeitos duradouros

São exemplos de medidas de integridade:

- Mudanças em sistemas e dados são autorizadas, por exemplo, um membro da equipe atribui um novo preço a um artigo no website e outro verifica a validade desse preço antes de ser publicado
- Onde possível, são criados mecanismos que forcem as pessoas a usar o termo correto
- As ações dos usuários são gravadas de forma que possa ser determinado quem modificou a informação
- Ações vitais para o sistema, como por exemplo, a instalação de software novo, não podem ser conduzidas por uma só pessoa. Ao segregar funções, posições e autoridades, ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências

A integridade dos dados pode ser garantida em grande parte por meio de técnicas de criptografia. Os princípios de política e de gestão para criptografia podem ser definidos em um documento de políticas separado

4.Disponibilidade

As características de disponibilidade são:

- **Oportunidade:** A informação está disponível quando necessário
- **Continuidade:** A equipe consegue continuar trabalhando no caso de falha
- **Robustez:** Existe a capacidade suficiente para permitir que toda a equipe trabalhe no sistema

Tanto uma falha de disco como um ataque de negação de serviço causam violação da disponibilidade. Qualquer atraso que exceda o nível de serviço esperado para um sistema pode ser descrito como uma violação da disponibilidade

A disponibilidade do sistema pode ser afetada pela falha de um dispositivo ou software. Dispositivos de backup devem ser utilizados para substituir rapidamente os sistemas críticos, e funcionários devem ser qualificados e estar disponíveis para fazer os ajustes necessários para restaurar o sistema. Questões ambientais também podem afetar a disponibilidade do sistema. Sistemas devem ser protegidos contra esses elementos, devidamente aterrados e monitorados de perto.

Ataques de negação de serviço (DoS) são métodos populares que hackers utilizam para interromper a disponibilidade e a utilização do sistema de uma empresa. Esses ataques são montados para impedir os usuários de acessar recursos e informações do sistema. Para se proteger desses ataques, apenas os serviços e portas necessárias devem estar disponíveis nos sistemas, e sistemas de detecção de intrusão (IDS) devem monitorar o tráfego da rede e a atividade das máquinas

Certas configurações de roteadores e firewalls também podem reduzir a ameaça de ataques DoS e possivelmente impedi-los de acontecer

Procedimentos de emergência são estabelecidos para garantir que as atividades possam ser recuperadas o mais breve possível após uma interrupção de larga escala.