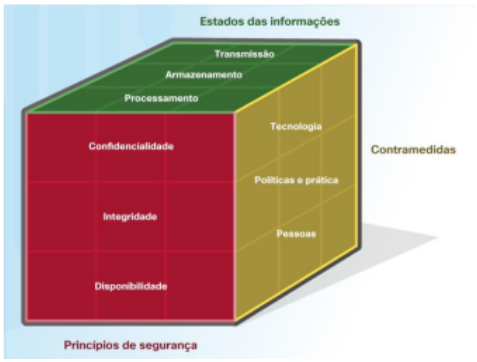
O cubo da segurança cibernética Part. 1 Primeira dimensão : Pilares da segurança da Informação

Data do Post	@August 9, 2021 9:00 AM (GMT)
Status	Done
Palavras-chave	Cubo da Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

John McCumber é um dos primeiros especialistas em segurança cibernética, desenvolveu uma estrutura chamada Cubo McCumber ou o cubo de segurança cibernética. Esse cubo é usado para gerenciar a proteção de redes, domínios e da Internet.



O cubo da segurança cibernética possui três dimensões:

- Primeira dimensão : Os três pilares da segurança da informação também denominada tríade CIA (confidentiality, integrity, availability).
- Segunda dimensão : Os três estados das informações ou dos dados - dados em repouso ou armazenados, dados em trânsito, dados em processamento
- Terceira dimensão : Contramedidas de proteção - Conhecimento necessário para proporcionar proteção

Primeira dimensão - pilares da segurança da informação

Os pilares da segurança da informação proporcionam foco e permitem ao especialista de segurança cibernética priorizar ações ao proteger qualquer sistema em rede. Esses pilares são confidencialidade, integridade e disponibilidade.

A confidencialidade impede a divulgação de informações para pessoas, recursos ou processos não autorizados. Integridade refere-se à precisão, consistência e confiabilidade dos dados. Finalmente, a disponibilidade garante que as informações estejam acessíveis para usuários autorizados quando necessário.

Abaixo começamos uma breve explanação sobre cada um dos pilares, começando pelo principio da confidencialidade.

Confidencialidade

A confidencialidade impede a divulgação de informações para pessoas, recursos ou processos não autorizados. A confidencialidade é associada a privacidade. A privacidade é o uso adequado dos dados. Quando as organizações coletam informações fornecidas pelos clientes ou funcionários, elas devem usar esses dados apenas para a finalidade a que se designam.

As empresas precisam treinar os funcionários sobre as melhores práticas para proteção de informações confidenciais, para se protegerem e também à organização, contra ataques. Os métodos usados para garantir a confidencialidade

incluem criptografia, autenticação e controle de acesso aos dados.

Proteção da privacidade de dados

As empresas armazenam uma grande quantidade de dados. Muitos desses dados armazenados são confidenciais. As informações confidenciais são dados protegidos contra acessos não autorizados para proteger um pessoas ou organizações. Há três tipos de informações confidenciais:

- **Informações pessoais** são informações de identificação pessoal (PII) de um determinado um indivíduo.
- **Informações comerciais** são informações que incluem qualquer coisa que representaa um risco para a empresa, se descoberta pelo público ou por um concorrente.
- **Informações confidenciais** são informações pertencentes a um órgão do governo, classificadas pelo seu nível de sensibilidade.

Controle de Acesso

O controle do acesso consiste em vários esquemas de proteção que impedem o acesso não autorizado a um computador, a uma rede, a um banco de dados ou a outros recursos de dados. Os conceitos de AAA envolvem três serviços de segurança: autenticação, autorização e accounting. Esses serviços proporcionam a estrutura principal para controlar o acesso.

Autenticação : serve para verificar a identidade de um usuário para evitar acesso não autorizado. Os usuários provam sua identidade com um nome de usuário ou um ID. Além disso, os usuários precisam verificar sua identidade proporcionando uma das opções a seguir.

- Algo que saibam (como uma senha)
- Algo que tenham (como um token ou cartão)
- Algo que sejam (como uma impressão digital)

Autorização : determinam quais recursos os usuários podem acessar, juntamente com as operações que os usuários podem executar. A autorização também pode controlar quando um usuário tem acesso a um recurso específico. Por exemplo, os funcionários podem ter acesso a um banco de dados de vendas durante o horário comercial, mas o sistema os bloqueia, depois de horas.

Accounting : permite ter o controle do que os usuários fazem, incluindo o que acessam, a quantidade de tempo que acessam os recursos e as alterações feitas. Por exemplo, um banco mantém o controle da conta de cada cliente. Uma auditoria do sistema pode revelar o tempo e o valor de todas as transações e o funcionário ou o sistema que executou as transações. Serviços de accounting de segurança cibernética funcionam da mesma maneira. O sistema controla cada transação de dados e fornece os resultados da auditoria. Um administrador pode configurar políticas de computador.

Integridade

A integridade é a precisão, a consistência e a confiabilidade dos dados durante todo o seu ciclo de vida. Um outro termo para integridade é qualidade. Os dados passam por várias operações, como captura, armazenamento, recuperação, atualização e transferência. Os dados 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, verificações de consistência dos dados e controles de acesso. Sistemas de integridade de dados podem incluir um ou mais dos métodos listados acima.

Necessidade de integridade de dados

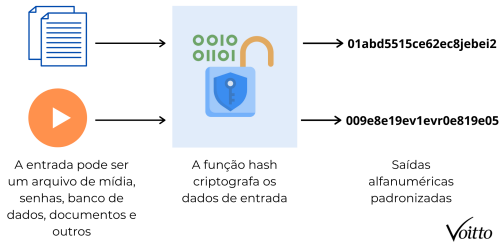
A integridade de dados é um componente fundamental da segurança da informação. A necessidade de integridade de dados varia, com base em como a organização usa os dados. Por exemplo, o Facebook não verifica os dados que um usuário publica em um perfil. Um banco ou organização financeira atribui uma importância mais alta à integridade de dados do que o Facebook. As transações e as contas de clientes devem ser precisas.

A proteção da integridade de dados é um desafio constante para a maioria das empresas. A perda da integridade de dados pode tornar recursos de dados inteiros não confiáveis ou inutilizáveis.

Verificações de integridade

Uma verificação de integridade é uma forma de medir a consistência de dados (um arquivo, uma foto ou um registro). A verificação de integridade realiza um processo chamado de função hash para tirar um retrato de dados em um momento específico. A verificação de integridade usa o snapshot para garantir que os dados permaneçam inalterados.

Uma soma de verificação é um exemplo de uma função hash. Uma soma de verificação verifica a integridade de arquivos, ou de strings de caracteres, antes e depois de serem transferidos de um dispositivo para outro por uma rede local ou pela Internet. As somas de verificação simplesmente convertem cada conjunto de informações para um valor e soma o total. Para testar a integridade de dados, um sistema de recebimento apenas repete o processo.



Funções hash comuns incluem MD5, SHA-1, SHA-256 e SHA-512. Essas funções hash usam algoritmos matemáticos complexos. O valor de hash está simplesmente ali para comparação. Por exemplo, depois de baixar um arquivo, o usuário pode verificar a integridade do arquivo, comparando os valores de hash da fonte com o valor gerado por qualquer calculadora de hash.

As empresas usam controle de versão para evitar alterações acidentais por usuários autorizados. Dois usuários não podem atualizar o mesmo objeto. Os objetos podem ser arquivos, registros de banco de dados ou transações. Por exemplo, o primeiro usuário a abrir um documento tem a permissão para alterar esse documento. A segunda pessoa tem uma versão somente leitura.

Backups precisos ajudam a manter a integridade de dados, se os dados forem corrompidos. Uma empresa precisa verificar o seu processo de backup para garantir a integridade do backup, antes que ocorra perda de dados.

A autorização determina quem tem acesso aos recursos da empresa, de acordo com a necessidade de cada um. Por exemplo, controles de acesso de usuário e permissões de arquivo garantem que apenas determinados usuários possam modificar os dados. Um administrador pode definir as permissões de um arquivo como somente leitura. Como resultado, um usuário que acessa esse arquivo não pode fazer nenhuma alteração.

Disponibilidade

A disponibilidade dos dados é o princípio usado para descrever a necessidade de manter a disponibilidade dos sistemas e serviços de informação o tempo todo. Ataques cibernéticos e falhas do sistema podem impedir o acesso a sistemas e serviços de informação. Por exemplo, a interrupção da disponibilidade do site de um concorrente por causa de um ataque pode proporcionar uma vantagem para seu rival. Ataques DoS (Denial-of-service, Negação de serviço) ameaçam a disponibilidade do sistema e impedem que usuários legítimos acessem e usem os sistemas de informações, quando necessário.

As organizações podem garantir a disponibilidade implementando o seguinte:

- Manutenção de equipamentos
- Atualizações do sistema e do SO
- Backups de teste
- Plano para desastres
- Implantam novas tecnologias
- Monitoramento de atividade incomum
- Teste para verificar a disponibilidade

Os cinco noves

As pessoas usam vários sistemas de informação em suas vidas diariamente. Computadores e sistemas de informação controlam a comunicação, o transporte e a fabricação de produtos. A disponibilidade contínua dos sistemas de informação é fundamental para a vida moderna. O termo alta disponibilidade descreve sistemas concebidos para evitar períodos de inatividade.

O objetivo é a capacidade de continuar a operar em condições extremas, como durante um ataque. Dentre as práticas mais populares de alta disponibilidade estão os cinco noves. Os cinco noves referem-se a 99,999%. Isso significa que o período de inatividade é menos de 5,26 minutos por ano.

Disponibilidade %	Tempo de inatividade
99.8%	17,52 horas
99,9% (“três noves”)	8,76 horas
99,99% (“quatro noves”)	52,56 minutos
99,999% (“cinco noves”)	5.256 minutos
99,9999% (“seis noves “)	31,56 segundos
99,99999% (“sete noves “)	3,16 segundos

Conclusões

Este artigo abordou a dimensão do cubo segurança cibernética pelo que, foi possível saber que ela está composta pelos três pilares da segurança da informação - confidencialidade, integridade e disponibilidade. Desse modo, esses três pilares ou princípios são a base para que os especialista da segurança cibernética possam gerenciar a proteção de redes, domínios e da Internet.