Princípios da Segurança, Testes de Vulnerabilidades, Ferramentas e Documentação

A Segurança da Informação está sobre os seguintes pilares, que devem ser garantidos por nós em nossas aplicações:

Autenticidade: Entende-se por autenticidade a certeza de que um objeto provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo. Na telecomunicação, uma mensagem será autêntica se for, de fato, recebida na íntegra, diretamente do emissor. Garante também o Não Repúdio.

Confidencialidade: A confidencialidade tem a ver com a privacidade dos dados da organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas. Faz com que a informação seja restrita e esteja somente disponível para usuários autorizados, é comum que as informações sejam categorizadas de acordo com o seu nível de criticidade, ou seja, a extensão do dano que poderia ser causado, caso fossem expostas e em função das medidas de segurança que precisam ser implementadas conforme essa característica.

Disponibilidade: Vamos ter acesso à informação quando precisarmos dela, sendo acesso a qualquer momento pelos colaboradores. Esse aspecto garante que as informações e os recursos estejam disponíveis para aqueles que precisam deles, 24 horas por dia, sete dias por semana. No mundo em que vivemos praticamente todos os processos de trabalho de uma empresa dependem de chegada ou busca de uma informação para acontecerem. Quando a informação está indisponível, os processos que dela dependem simplesmente ficam paralisados. Caso haja indisponibilidade de um conjunto grande ou especificamente crítico de informações, a empresa pode parar e entrar em estado de lucro cessante, quando não de prejuízo.

Integridade: significa garantir que a informação armazenada ou transferida está correta e é apresentada corretamente para quem a consulta. Esse pilar pode ser menos emocionante, mas é absolutamente crítico do ponto de vista operacional, pois valida todo o processo de comunicação em uma empresa ou comunidade. Esse princípio garante que as informações, tanto em sistemas subjacentes quanto em bancos de dados, estejam em um formato verdadeiro e correto para seus propósitos originais. Logo, o receptor da informação detém as mesmas informações que o seu criador.

Dessa forma, a informação pode ser editada apenas por pessoas autorizadas e permanece em seu estado original quando não for acessada. Assim como a confidencialidade de dados, a integridade é implementada usando mecanismos de segurança, como criptografia e hashing.

Apesar de ela ser garantida por política de controles de acesso, as alterações nos dados também podem ocorrer como resultado de eventos não causados por humanos, como pulso eletromagnético ou falhas do servidor, sendo imprescindível manter procedimentos seguros

de backup e adotar na infraestrutura de TI sistemas com configuração redundante.

Um exemplo de integridade utilizado por muitas ferramentas, é o "hash de mão única", também conhecido como:

- Checagem de redundância cíclica;
- Função de hash universal;
- checksum criptográfico;

Legalidade: Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
Estes princípios podem ser comprometidos com possíveis ameaças, físicas ou lógicas.

Análise de Vulnerabilidades

Análises de vulnerabilidade identificam, quantificam e priorizam o que há de mais frágil nos seus sistemas, a fim de tornar sua segurança mais robusta. E, embora sejam tradicionalmente executadas em ambientes de TI, elas não se limitam a essa aplicação.

É possível fazer uma análise de vulnerabilidade em sistemas elétricos ou de comunicação, por exemplo. Além disso, tanto os pequenos quanto os grandes negócios podem se beneficiar dela.

Uma análise de vulnerabilidade é diferente de um teste de penetração porque seus objetivos são distintos. Enquanto o teste explora táticas específicas de invasão, a análise identifica todas as brechas existentes em um sistema.

Tipos de Análises de Vulnerabilidade

- Black box
    - Sem conhecimento da estrutura
- White box
    - Com conhecimento da estrutura
- Gray box
    - Conhecimento parcial

Análise de Vulnerabilidades - Planejamento

- Informações gerais
- Contrato de acordo
- Objetivo da Análise
- Limitações
- Linha do tempo (Relatórios)

Fases da Análise de Vulnerabilidades

- Reconhecimento (Footprint)
- Varredura (Scanning)
- Exploração (Gaining Access)
- Escalação de Privilégios (Maintaining Access)

Metodologias para Análise de Vulnerabilidades

Existem vários tipos de metodologias que podem ser aplicadas na Análise de Vulnerabilidades. Cada uma atende à necessidades específicas, algumas destas são:

- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- WASC-TC (Web Application Security Consortium Threat Classification)
- OWASP (Open Web Application Security Project)