Ameaça, Vulnerabilidade, Impacto e Controle

Roteiros e tópicos para estudo por

Vinícius da Silveira Serafim
professor@serafim.eti.br
http://professor.serafim.eti.br

Palavras-chave: vulnerabilidade, ameaça, impacto e controle

Considerações iniciais

Para compreendermos um ataque, precisamos necessariamente compreender o significado dos seguintes conceitos:

- Ameaça
- Vulnerabilidade
- Impacto
- Controle

Mas para de fato compreendermos um ataque temos ainda que estudar um pouco sobre os atacantes. (próximo roteiro)

Todo o conteúdo deste roteiro (e desta aula) tem caráter introdutório. Todos os conceitos serão trabalhados com maior profundidade ao longo das aulas.

Ameaça

Definição

Um conjunto de circunstâncias que têm o potencial de causar uma quebra da segurança. (PFLEEGER, 2006, p.15)

Explicação

Uma ameaça poder ser de origem humana, por exemplo, sendo decorrente de uma ação intencional (ataque) ou não (um erro de operação). Os desastres naturais também são ameaças como, por exemplo, enchentes, descargas elétricas, terremotos, etc.

Um exemplo de uma ameaça humana e intencional é um atacante (cracker) contratado por uma empresa concorrente para atingir a empresa alvo.

Uma sobrecarga de energia, por exemplo, pode ser causada por uma ação humana não intencional (operador da empresa distribuidora de energia), por uma ação humana intencional (atacante que invadiu uma central de controle) ou simplesmente pela queda

de um raio. Porém, no final das contas, simplesmente temos que proteger os ativos contra uma eventual sobrecarga de energia.

Vulnerabilidade

Definição

É uma propriedade de um ativo ou do seu ambiente que, em conjunto com uma ameaça, pode levar a uma falha da segurança. (ANDERSON, 2008, p.15)

Explicação

Vamos direto a um exemplo bem simples: as informações armazenadas em um sistema estão sujeitas à manipulação (cópia, alteração, deleção,...) não autorizada por não haver nenhum mecanismo de autenticação de usuários.

Nesse caso a ameaça é: manipulação não autorizada de dados. E a vulnerabilidade é: ausência de mecanismo de autenticação de usuários.

Estudaremos algumas vulnerabilidades bastante comuns na aula 7 (Falhas em programas e códigos maliciosos).

Impacto

Definição

O impacto é o resultado de uma ameaça concretizada, ou que veio a ocorrer.

Explicação

No exemplo anterior, citado na *vulnerabilidade*, qual seria o impacto para a empresa (ou organização) de ter informações copiadas por um funcionário (atacante) e entregues ao concorrente ou simplesmente publicadas na Internet? É claro que a resposta depende fundamentalmente das particularidades do negócio da empresa (ou organização) e das informações copiadas. Alguns exemplos:

- Empresa: hospital
  - Informações: fichas de pacientes internados foram publicadas na Internet
  - Impacto: responsabilização legal, dano à imagem, perda de pacientes

- Empresa: banco
  - Informações: saldos de correntistas “premium” entregue ao banco concorrente
  - Impacto: perda de clientes, quebra de sigilo bancário (impacto legal)

Memorizando ameaça, vulnerabilidade e impacto

Para facilitar a compreensão e evitar confusões na hora de identificar qual é qual, você pode associar cada uma das três definições à perguntas:

- Ameaça: O que pode acontecer?
- Vulnerabilidade: Por que pode acontecer?
- Impacto: Qual é o resultado se acontecer?

Ao ter uma situação em análise vá respondendo às perguntas. Retomando o exemplo utilizado ao longo do roteiro, vamos responder às perguntas:

- O que pode acontecer? *Manipulação não autorizada de informações*
- Por que pode acontecer? *Porque o sistema não implementa nenhum mecanismo de autenticação de usuários*;
- Qual é o resultado se acontecer? *Responsabilização legal, dano à imagem e perda de pacientes*. (no caso do hospital).

Resta alguma dúvida de qual é a ameaça, a vulnerabilidade e o impacto? Se sim, entre em contato comigo. ;)

Controle

Definição

Uma ação, dispositivo, procedimento ou técnica que remove ou reduz uma vulnerabilidade. (PFLEEGER, 2006, p.15)

Explicação

Acreditando que a definição já é bem clara, vou seguir com os exemplos.

- Firewall: é um dispositivo que visa filtrar e registrar as comunicações entre domínios de segurança diferentes como, por exemplo, entre a Internet e a rede interna de uma empresa. Com esse controle, por exemplo, é possível isolar (ao menos diretamente) um servidor de banco de dados da Internet.
- Autenticação de usuários: dispositivo que visa reduzir a vulnerabilidade de um sistema impedindo que pessoas não autorizadas obtenham acesso às informações nele armazenadas.

Pfleeger em (PFLEEGER, 2007, p.7) afirma: “Uma ameaça é bloqueada pelo controle de uma vulnerabilidade”. Em outras palavras, elimine ou reduza vulnerabilidades e você estará reduzindo as chances de uma ameaça se concretizar.

Exercícios

Se você tentar responder venha falar comigo para vermos se suas soluções estão corretas. Não é importante que você acerte todas, mas é muito interessante que você tente responder à todas as perguntas.

1) Considere um ambiente ou sistema que você conheça e liste ao menos 5 *ameaças*.

2) Para cada uma das ameaças listadas, descreva sucintamente um possível impacto para o negócio.

3) Para cada uma das ameaças listadas, descreva uma vulnerabilidade que possibilitaria sua ocorrência. (não se preocupe em saber se a vulnerabilidade existe ou não de fato no ambiente que você considerou na questão 1)

4) Procure indicar um controle para eliminar, ou reduzir, cada uma das vulnerabilidades que você listou.

5) Considere a seguinte situação e responda à pergunta ao final: uma empresa tem sofrido prejuízos financeiros e, eventualmente, desgaste com clientes devido ao lançamento de valores de cobrança errados no sistema ERP; a causa desses erros é falta de treinamento para os usuários. Qual é a ameaça, a vulnerabilidade e o impacto?

Bibliografia

ANDERSON, R. J. Security Engineering: A Guide to Building Dependable Distributed Systems. 2a edição. Wiley, 14 de abril de 2008. 1080 pág.

PFLEEGER, C. P. Security in Computing. 4a edição. Prentice Hall, 23 de outubro de 2006. 880 pág.