Aula 9 TP – 01/abril/2019

Grupo 3

1. Vulnerabilidades de Codificação

- ***Pergunta 1.1***

1) Estima-se que qualquer pacote de software tem uma média de 5 a 50 bugs por cada 1.000 linhas de código fonte. Assim concluímos:

  - Facebook com 62 milhões SLOC, terá entre 310 mil a 3 milhões e 100 mil bugs.
  - Car Software com 100 milhões SLOC, terá entre 500 mil a 5 milhões de bugs.
  - Linux 3.1 com 15 milhões SLOC, terá entre 75 mil a 750 mil bugs.
  - Google (all services) com 2 biliões SLOC, terá entre 10 milhões a 100 milhões de bugs.

2) É impossível saber quantas vulnerabilidades existem exatamente num determinado número de bugs.

- ***Pergunta 1.2***

Vulnerabilidades de projeto: por exemplo, erros na conceção da arquitetura ou uma má implementação de protocolos criptográficos. Estas vulnerabilidades podem por em causa toda a reestruturação do projeto, sendo que mediante a fase em que este se encontra, podem representar custos elevados.

Vulnerabilidades de codificação: por exemplo, utilizar software criado por outras entidades ou *buffer overflow*. Dependendo do tipo de bug e da informação sobre o software, a correção destas vulnerabilidades pode ser mais fácil do que as vulnerabilidades anteriores.

Vulnerabilidades operacionais: por exemplo, dificuldade na aplicação das *patch* ou utilização de um sistema operativo vulnerável. Quando um utilizador usa um software num sistema operativo vulnerável, então esse mesmo software também fica sujeito a certas vulnerabilidades. Neste caso as correções serão através das *patch*, porém esta ação depende do utilizador, o que torna bastante complicado o controlo da correção efetuada.

- ***Pergunta 1.3***

O que distingue uma *vulnerabilidade dia-zero* de outra *vulnerabilidade de* codificação *que não seja de dia-zero* é o facto de a primeira não ser do conhecimento da empresa que está a desenvolver o software. Este tipo de vulnerabilidades *dia-zero* leva a que não seja possível aplicar um *patch* (uma correção) e como consequência o sistema que a possui poderá ser alvo de ataques (*zero day attack*). As vulnerabilidades de codificação que não sejam dia-zero são aquelas conhecidas pela empresa, contudo podem de imediato resolver o problema de maneira a não sofrerem ataques.