### **ATIVIDADE - THREAT MODELING**

**Objetivo**

O objetivo desta atividade é praticar o *threat modeling* utilizando as categorias determinadas pelo STRIDE. O software a ser modelado será o Dropbox.

**Material**

Você pode instalar uma ferramenta para *threat modeling* como o OWASP ThreatDragon (https://owasp.org/www-project-threat-dragon/docs-1/introduction/) ou o Microsoft Threat Modeling Tool (<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>). O Microsoft Threat Modeling Tool é mais popular, enquanto o ThreatDragon tem opções para sistemas operacionais diferentes, além de uma versão Web. Também é possível fazer os diagramas e a documentação usando uma ferramenta como o draw.io e uma planilha.

**Sobre o Dropbox**

O Dropbox (https://www.dropbox.com/) é uma ferramenta de armazenamento de arquivos na nuvem. Ela pode ser utilizada a partir de PCs ou dispositivos móveis. Quando o usuário cria um novo arquivo em seu repositório Dropbox local, este novo conteúdo é imediatamente enviado para o servidor na nuvem e a modificação é sincronizada em todos os dispositivos conectados a esta conta de usuário. Além disso, as modificações são registradas em uma espécie de controle de versão, de forma que versões anteriores dos arquivos possam ser restauradas.

Uma das funcionalidades mais interessantes do Dropbox é a *de-duplication engine*. Os clientes mantém uma lista local de hashes de todos os arquivos contidos em sua pasta Dropbox. Quando um arquivo é alterado, o Dropbox recalcula o código hash do arquivo, e envia todos os hashes para o servidor. O servidor, por sua vez, aplica a seguinte lógica a cada hash:

* nova mudança: se o servidor não tem este hash, o arquivo é enviado ao servidor.
* sem mudança: se o servidor já tem esse código hash atrelado a este usuário, o arquivo não é enviado ao servidor.
* de-duplicate: se o servidor já tem este hash, mas ele está atrelado a outro usuário, então é criada uma entrada no servidor apenas registrando que o usuário atual mantém uma cópia deste arquivo em seu computador. Em suma, neste caso, o arquivo não é enviado ao servidor.

O *de-duplication* economiza bastante tempo em termos de envio de arquivos e espaço de armazenamento nos servidores do Dropbox.

Por fim, os servidores do Dropbox estão distribuídos geograficamente e os dados são replicados nestes diversos locais para oferecer confiabilidade e maior desempenho. Estes servidores replicados são gerenciados por um único sistema gerenciador de banco de dados. Todos os clientes (desktop, dispositivos móveis e web) interagem com a mesma API.

**Atividade**

1- Pense rapidamente sobre a arquitetura do sistema. Faça um esboço em papel colocando os principais componentes conforme a descrição acima.

2- Inicialize a ferramenta de *threat modeling* que você instalou ou o draw.io. Crie um novo diagrama em branco.

3- Comece a desenhar a arquitetura criando *data stores*, *processes*, e *external interactors*.

4- Adicione as relações de fluxo de dados. Você deve dar nome a todas estas relações utilizando verbos (por exemplo, “envia arquivo”).

5- Adicione os machine boundaries e os trust boundaries.

6- Para cada um dos elementos no diagrama, cadastre duas ameaças. Ao final, devemos ter ao menos uma ameaça para cada um dos tipos STRIDE. Dica: recorra às notas de aula para verificar os tipos de ameaças mais comuns para cada tipo de elemento. Utilize também o livro “Playbook for threat modeling of medical devices”; no Apêndice A.1 deste livro, há um exemplo bem detalhado de threat modeling utilizando o STRIDE.

7- Para cada uma das ameaças, descreva uma possível solução de mitigação.

8- Discutir os resultados com o restante da sala.

9- Submeta o arquivo com o resultado na atividade do Google Classroom.