Faculdade de Design,
Tecnologia e Comunicação
Universidade Europeia

Sistemas Distribuídos
Anti-Ransomware

João Rolo
Tomás Ferreira
Martim Costa

GitHub: https://github.com/tolojo/Anti-Ransomware-SD

1. Descrição do Problema

Uma modificação não autorizada de um sistema de ficheiros é algo que se deseja evitar, seja devido a ataques de ransomware ou outra causa.

O que pretendemos com este trabalho é criar um sistema que seja tolerante a falhas, eficaz e escalável.

O que nos levou a escolher este tema é o facto do projeto da unidade curricular Project Factory trabalhar com dados que são sensíveis e que não podem ser alterados no sistema por terceiros, desta forma iremos implementar o nosso próprio sistema de anti-ransomware, de forma a ter um maior entendimento de como este tipo de software funciona.

2. Casos de Uso

- Autenticação no sistema;
- Alteração de ficheiros por um utilizador autorizado;
- Alteração de ficheiros por um utilizador não autorizado;
- Deteção e recuperação de ficheiros corrompidos.

3. Solução a Implementar

Todos os ficheiros vão estar guardados num banco de dados que é replicado (dois bancos de dados ativos em simultâneo), cuja alteração só será permitida a utilizadores autenticados. Estes ficheiros vão ser encriptados com uma Hash Function (SHA-256) e a chave resultante da função vai ser guardada num banco de dados que não é acedido pelos utilizadores, juntamente com uma cópia do ficheiro que está contido no banco de dados dos clientes.

A função SHA-256 é uma variante do SHA-2 que consiste em transformar um tamanho arbitrário de dados e mapeá-lo para dados de um tamanho físico o que irá servir para verificar a integridade dos ficheiros.

Para o nosso sistema, sempre que um utilizador autenticado efetuar uma alteração em algum ficheiro irá atualizar automaticamente a Hash Key resultante da função SHA-256 e irá atualizar também a cópia de segurança do ficheiro contido no banco de dados dos clientes. Desta forma, se um utilizador não autenticado efetuar alguma alteração no sistema a Hash Key não será modificada e será detetada a alteração indevida de dados.

4. Enquadramento nas Áreas da Unidade Curricular

Em termos da disciplina de Sistemas Distribuídos é disponibilizada uma divisão da carga de trabalho por parte dos servidores, tal como das bases de dados, aumentando assim a eficácia e tornando-a mais tolerante a falhas.

Um Sistema Distribuído vai permitir que na ocorrência de algum erro ou atualização no banco de dados ou no servidor a aplicação não irá pôr em risco a operacionalidade do sistema.

Do ponto de vista de sincronismo do sistema é necessário saber que dados são necessários manter e quais são necessários alterar quando estes estão em concorrência.

Relativamente à segurança dos ficheiros é indispensável existir uma forma detetar ficheiros corrompidos ou indevidamente alterados, como também uma forma de recuperar os mesmos de forma a manter a integridade do sistema. Assim a autenticação 2 fatores será crucial para garantir que apenas utilizadores autenticados possam alterar os dados dos ficheiros.

5. Requisitos Técnicos

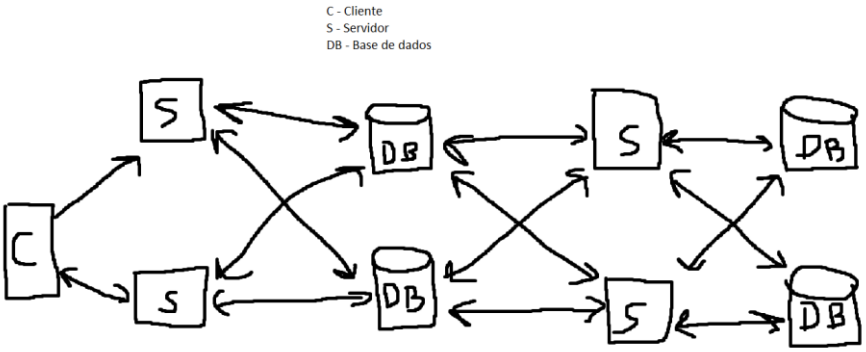
O sistema irá ter 2 servidores de comunicação com o cliente, 2 sistemas de bases de dados replicados, 2 servidores que se encarregam da encriptação das bases de dados e duas bases de dados seguras, que apenas o servidor de encriptação vai ter acesso, onde vão estar guardadas as Hash Keys e uma cópia de segurança dos ficheiros.

6. Arquitetura da Solução

A arquitetura do sistema vai consistir num cliente web para proceder a ligação com os servidores, dois servidores que estarão a funcionar em simultâneo, dois bancos de dados que serão acessíveis pelos utilizadores, um servidor que vai ser responsável pela verificação da integridade dos ficheiros, e um banco de dados que

vai guardar as Hash Keys dos ficheiros e uma cópia de segurança dos ficheiros contidos nos bancos de dados.

Os servidores necessitam de ter no mínimo 512mb de memoria RAM e 4gb de memoria ROM.



7. Tecnologias

8. Bibliografia

https://www.n-able.com/blog/sha-256-encryption
https://www.notion.so/product