David Grunheidt Vilela Ordine - 16202253

INE5429 - 2021.2 - Trabalho Pensamento de Segurança

Universidade Federal de Santa Catarina

Departamento de Informática e Estatística

Ciência da Computação

Florianópolis

2021

Sumário

1 Sistema analisado

Neste trabalho serão analisadas questões de segurança sobre o Firebase, ferramenta de computação em *cloud* utilizada por diversas aplicações, a qual prove soluções como funções que rodam diretamente na *cloud*, análises de uso de aplicativos através de eventos, notificações *push*, configurações remotas do *app* sem necessidade de fazer *release* e muitos outros serviços

1.0.1 Ativos

Um sistema como o Firebase lida com questões de segurança em uma complexidade de escala enorme. Desde a parte da autenticação de usuários para o acesso a determinados projetos, o uso de permissões para que estes usuários só possam acessar certos serviços, até a parte de validação de que um determinado projeto está associado a alguma aplicação e essa associação não pode ser alterada para outra aplicação. Caso um acesso caia nas mãos erradas, muita coisa pode ser feita em relação a uma aplicação, como acessar dados sensíveis, alterar registros em banco de dados, mandar notificações com conteúdo malicioso ou inutilizar completamente algum serviço alterando propriedades cruciais deste.

Como citado acima, o Firebase possui muitos serviços, e alguns são precificados conforme o uso de um certo projeto. Estes serviços devem apresentar uma alta disponibilidade para que o usuário final veja valor em utiliza-los. Logo, na visão do autor deste trabalho 4 ativos podem ser listados como de maior importância:

1. **Restrição de acesso aos projetos e serviços dentro de uma organização.**
    - Um usuário de uma organização deve ter acesso a somente alguns projetos desta. Além disso, dentro destes projetos, podem existir serviços em que o usuário não esteja habilitado a usar.
2. **Privacidade das informações de acesso dos usuários.**
    - As informações de acesso dos usuários, como login, senha, organizações que está associado, nome, localidade, informações de pagamento, etc.
3. **Precificação de serviços e medição do uso destes serviços.**
    - Alguns serviços dentro do Firebase são pagos, por exemplo, o *Cloud Firestore*. Portanto, é necessário medir e cobrar o uso destes serviços.
4. **Disponibilidade dos serviços.**

1.0.2 Adversários

Os adversários que podem querer violar a segurança de cada um dos ativos variam conforme o ativo. Abaixo são feitas descrições mais detalhadas sobre os perfis dos diferentes adversários conforme o ativo relacionado a eles.

1.0.2.1 Ativo 1: Restrição de acesso aos projetos e serviços

Este ativo possui o adversário mais importante, pois ele é uma pessoa que tem acesso de administrador da organização ou de um projeto dentro da organização. Muitas vezes, por **desleixo ou negligência**, esse adversário cria novos usuários para integrantes da equipe com nível de experiência básica e esquece de configurar as permissões corretamente para prevenir que estes usuários façam alguma ação indevida. Essas ações indevidas incluem a exploração dos serviços e clique em botões sem saber o que aquilo realmente faz ou ações maliciosas por vingança após algum integrante ser demitido e o adversário não desassociar sua conta a tempo.

1.0.2.2 Ativo 2: Privacidade das informações de acesso dos usuários

O perfil desse adversário está mais voltado a *hackers* que não possuem acesso especifico a alguma organização e/ou projeto. Esses adversários estão interessados em obter as informações sigilosas com ou sem foco em alguma empresa, para que, com essas informações, consigam acessar um projeto e realizar ações indevidas, como mandar uma notificação sem sentido para alguma aplicação ou inviabilizar o uso da aplicação ao apagar totalmente os dados armazenados no Firestore

1.0.2.3 Ativo 3: Precificação de serviços e medição do uso destes serviços

O perfil desse adversário é um *hacker* que possui acesso a alguma organização e projeto especifico. Esse adversário quer burlar o sistema de precificação do Firebase para que as medições sobre os serviços utilizados por suas aplicações tenham um valor errado, resultando em reduções sobre o custo total de uso destes serviços.

1.0.2.4 Ativo 4: Disponibilidade dos serviços.

O perfil desse adversário também é um *hacker*, não importando se este tem ou não acesso a alguma organização e projeto no Firebase. Esse adversário quer inviabilizar por completo algum dos serviços do Firebase, como o *Cloud Messaging*, para que nenhuma aplicação consiga mandar uma notificação *push* durante um período de tempo, ou o *Cloud Firestore*, o que inviabilizaria a utilização de centenas de milhares aplicações que utilizam esse serviço para armazenar seus dados e mostra-los no *front-end* para o usuário final. Esse adversário é o mais perigoso de todos, pois possui as intenções mais maliciosas.

2 Gerenciamento de Risco

Os ativos citados na seção 1.0.1 possuem probabilidades de acontecer e impactos caso aconteçam diferentes. Assim, essas informações foram reunidas na tabela abaixo para melhor visualização.

Ataque ao ativo	**Probabilidade**	**Impacto**
Restrição de acesso	Alta	Alto
Privacidade das informações de acesso	Média	Variado
Precificação e medição de serviços	Baixa	Baixo
Disponibilidade dos serviços	Baixa	Alto

O ativo de restrição de acesso tem alta probabilidade de acontecer, visto que nem todas as empresas se preocupam em contratar pessoas qualificadas para atuar como administradores de serviços em *cloud*. Essas pessoas esquecem ou simplesmente não fazem o gerenciamento correto dos acessos por diversos motivos, como má vontade, preguiça ou falta de experiência. Seu impacto também é alto pois pode acarretar em situações catastróficas para a empresa, como o não funcionamento de algum modulo crítico que utiliza algum serviço do Firebase.

O ativo de privacidade das informações de acesso tem média probabilidade de acontecer pois depende da experiência dos usuários com acesso ao Firebase e do conhecimento desses usuários sobre o impacto do vazamento de informações sobre seu acesso. Usuários pouco cuidados podem compartilhar seu acesso com alguém fora da equipe ou com alguém da equipe que não deveria ter essa informação, tornando a chance deste acesso cair em mãos erradas muito maior. Usuários podem também armazenas suas informações de acesso em plataformas pouco confiáveis e, mesmo que seja muito difícil um *hacker* invadir um sistema tão complexo como o Firebase, **da Google**, pode ser muito mais fácil pra ele invadir a plataforma simples que o usuário armazenou suas informações de acesso. Seu impacto também é variado pois depende do nível de permissão do acesso que foi invadido, já que, em um certo projeto, existirão acessos com poucas ou nenhuma permissão e acessos com muitas permissões a sistemas críticos.

O ativo de precificação e medição de serviços tem baixa probabilidade pois as ferramentas da Google, incluindo o Firebase, são largamente conhecidos por sua robustez e resiliência, sendo praticamente impossíveis de serem invadidos. Burlar a precificação do uso de serviços do Firebase seria uma tarefa extremamente difícil para qualquer pessoa, e, se feita num contexto de organização, seria vista com maus olhos pelos demais integrantes, podendo até acarretar em demissão. O impacto deste ativo também seria baixo, pois, mesmo que alguém conseguisse burlar a precificação, seria uma pessoa entre centenas de milha-

res de outras que pagam regularmente a Google, sem falar que essa brecha duraria somente algumas horas antes de alguém do time da Google descobrir sobre.

Pelo mesmo motivo do ativo acima, o ativo de Disponibilidade dos serviços tem baixa probabilidade de acontecer. Porém diferente do ativo acima, o impacto caso um *hacker* consiga negar a disponibilidade de um dos serviços do Firebase seria enorme, pois estaríamos falando na paralisação de módulos de todas as aplicações (centenas de milhares) que utilizam este serviço. Outro resultado direto da paralisação de um serviço seria a diminuição nos ganhos da Google por um período de tempo, o que contribui também para a classificação do impacto como alto.

2.0.1 Contra medidas

Para o ativo de restrição de acesso, as empresas que fornecem serviços em *cloud* possuem artigos detalhando as melhores práticas em relação as configurações de acesso das suas ferramentas, como essas recomendações da AWS ou essas instruções da GCP. Essas empresas também possuem artigos ensinando o que fazer quando um usuário com acessos é demitido ou sai da empresa, por exemplo, esse artigo da Google que serve também para o Firebase, esse tutorial da Microsoft ou esse passo-a-passo da Tech Republic. Portanto, esses artigos podem ser passados aos administradores com menos experiência na configuração de permissões para que eles tenham um ponto de partida e consigam proteger melhor o sistema que trabalham.

Já para o ativo de privacidade das informações de acesso a empresa pode estabelecer, através de um contrato assinado na contratação do integrante, politicas duras quanto ao compartilhamento de informações **privadas** com outras pessoas, estabelecendo punições caso algo assim venha a ser descoberto, o que irá desencorajar os seus integrantes a fazerem isso. Quanto ao Firebase, é esperado que este armazene informações sigilosas, como a senha do usuário, em um formato criptografado e irreversível, de modo que mesmo que alguém consiga extrair essas informações, não consiga acessar alguma conta de usuário.

Para o ativo de precificação e medição de serviços, que atinge diretamente o Firebase como o todo, sistemas redundantes de monitoramento podem ser de grande ajuda para detectar possíveis contradições de preços e provavelmente a Google já deve ter algo assim implementado. Além disso, politicas duras para quem tentar aplicar tais golpes, com banimento da plataforma ou processo, podem ser aplicadas nos termos de uso, desencorajando tais atos.

Por fim, para o ativo de Disponibilidade dos serviços a Google também é conhecida por possuir ferramentas com alta disponibilidade, incluindo o Firebase, como é possível ver nesse relatório de *status* dos seus serviços nos últimos anos ou neste documento, o qual garante mais de 99% de disponibilidade no serviço de *Cloud Storage*. Portanto, pode-se dizer

que as contra medidas necessárias já estão sendo aplicadas, mas como exemplo podemos citar o espalhamento de servidores em continentes distintos e países distintos como forma de se prevenir contra desastres naturais ou ataques terroristas.

2.0.2 Custo/Benefício

Assim como no capítulo 2, as contra medidas de ataque aos ativos citadas na seção 2.0.1 possuem custos e benefícios diferentes. Essas informações foram concentradas na tabela abaixo para melhor visualização.

Contra medida ao ativo	**Custo**	**Benéfico**
Restrição de acesso	Baixo	Alto
Privacidade das informações de acesso	Baixo	Alto
Precificação e medição de serviços	Médio	Médio
Disponibilidade dos serviços	Altíssimo	Altíssimo

Como é possível ver, todas as contra medidas tem uma importância considerável. A menor delas na visão do autor seria a contra medida ao ativo de precificação de serviços, pelo impacto de um ataque neste ativo ser de baixo nível. As duas primeiras contra medidas são facílimas de implementar, pois envolvem basicamente uma conversa e algumas linhas no contrato, e o custo só não foi reduzido a zero pois, para conversar com alguém sobre uma regra são gastos o tempo das 2 pessoas da conversa, o que implica num custo, e, para definir questões em contrato é necessário contratar um advogado para a empresa.

O ativo de disponibilidade de serviços tem um custo altíssimo pois apresenta uma complexidade gigantesca, envolvendo questões de implementação de várias áreas diferentes dentro da computação, por exemplo, a área de computação distribuída. O beneficio de ter alta disponibilidade também é gigantesco, pois constrói uma imagem positiva da empresa e atrai mais consumidores para esta, aumentando seus ganhos no longo prazo.