Cartilha de Boas Práticas de Segurança

Fiéis à missão de aprimorar a segurança e a qualidade da operação, é com prazer que compartilhamos com você essa cartilha de Boas Práticas de Segurança, que compila uma lista de 10 dicas que a sua organização poderá implementar para mitigar riscos, proteger-se de fraudes digitais e operar no nível de serviço que anseiam.

1- Responsabilidade sobre a credencial de acesso
A credencial de acesso é a chave que torna possível o acesso de usuários aos sites do Fitbank e a integração de sistemas (cliente x FitBank), fornecendo os serviços de autenticação e identificação das operações. Cuidar da guarda e manter a confidencialidade da credencial cuidando para que a mesma não seja divulgada ou compartilhada, são responsabilidades exclusivas do cliente.

2- Não Compartilhar sua credencial
Em hipótese nenhuma sua credencial pode ser compartilhada. Ao compartilhar sua credencial. você está permitindo que outro usuário use a sua identificação para acessar sites e realizar chamadas na API, possibilitando acesso e controle total dos recursos disponibilizados, comprometendo assim a operação e a rastreabilidade proporcionada pela credencial e, obviamente, facilitando a fraude.

3 – Não divulgar sua credencial
Em hipótese nenhuma sua credencial deve ser guardada ou transmitida em texto claro (não criptografado), mesmo em mídias internas ou em canais de comunicação internos, como e-mails. Também é importante cuidar para que arquivos de configuração de aplicações ou scripts sejam protegidos contra visualizações indevidas se for o caso deles armazenarem credenciais. Adicionalmente, utilize apenas requisições POST via HTTPs para transmitir credenciais de autenticação para nossas APIs.

4 – Não armazenar sua credencial em código de aplicações
Se a sua empresa desenvolve códigos e scripts para acessar nossas APIs você deve ficar atento para nunca armazenar credenciais em código fonte ou em código compilado pois os desenvolvedores podem usar o GitHub ou outros repositórios de código aberto como um meio de colaborar entre si e concluir projetos e isso pode significar que suas credenciais ficarão expostas para o mundo inteiro.

5 – Uso de cofre de credenciais
Aconselhamos o uso de um serviço de nuvem para armazenar e acessar segredos de maneira segura. Um segredo é qualquer coisa a qual você queira controlar rigidamente o acesso, como chaves de API, senhas, certificados ou chaves criptográficas. Existem diversas opções no mercado como AWS Certificate Manager, Azure Key Vault e HashiCorp Vault.

6- Rotacionamento de credencial
O rotacionamento das credenciais é essencial para aumentar o nível de segurança de credenciais de acesso, sendo uma ação prioritária dentro das políticas e boas práticas recomendadas. O rotacionamento de sua credencial pode ser feito de forma programática usando uma chamada
API:

```
{
 "Method": "GenerateNewCredentials",
 "PartnerId": "xxxx",
 "BusinessUnitId": "xxxx"
}
```

É de extrema importância o cuidado ao gerar novas credenciais, dada a necessidade de atualização nos sistemas e scripts que fazem referência à chave antiga. Se possível, o rotacionamento deve ser executado através do cofre de credenciais de forma a evitar que terceiros tenham acesso ao retorno da chamada.

7 – Utilização de endereço IP fixo.

Um endereço IP é um código numérico que vincula individualmente um dispositivo ou uma interface a rede Internet. Quando utilizado apenas um IP, o chamado IP Fixo, entrega com certeza a identificação do cliente que está acessando nossos recursos, promovendo a segurança, facilitando a monitoria e evitando bloqueios e restrições no acesso a API. Ademais, o uso de uma credencial pode ser mapeado para o IP fixo indicado pelo cliente, evitando que credenciais roubadas sejam usadas por terceiros. Embora não seja obrigatório, o uso de um endereço IP fixo para acesso às nossas APIs públicas é altamente encorajado.

8 – Uso de duplo fator de autenticação (2FA)

A autenticação de dois fatores é uma camada extra de proteção que pode ser ativada em contas online. O recurso insere uma segunda verificação de identidade do usuário no momento do login, evitando o acesso às contas mesmo quando a senha é vazada. O uso desse recurso é encorajado caso o cliente use aplicativos móveis e websites desenvolvidos internamente como *frontend* para as nossas APIs.

9 – *Logging* de atividades e operações

Todos os acessos feitos às nossas APIs e web sites são logados garantindo a rastreabilidade das operações. Todas as operações podem ser rastreadas por data e horário de execução, por IP de origem, pela URL e pela URL Path acessadas. Além disso podemos ver quantas e quais operações foram executadas, que deram falha (e quais falhas), etc. Encorajamos que você também faça o *logging* de suas atividades. Comparar os logs de atividade enviados e recebidos é uma forma comum de *debug* de operações e também serve para análises de segurança (quando uma das partes detecta um comportamento anômalo).

10 – Avaliar sua própria segurança

É imperativo que você avalie a segurança do seu departamento de TI pelo menos uma vez a cada semestre. Essa avaliação pode ser feita por seu time interno de segurança da informação ou por um time de especialistas externo. Também é aconselhável que você tenha implementada alguma ferramenta capaz de avaliar e apontar as vulnerabilidades presentes no seu parque de informática, como por exemplo, sistemas operacionais desatualizados, softwares vulneráveis etc. É importante salientar que a avaliação interna de risco é uma deliberação prevista em diversos órgãos reguladores, como o BACEN, a CVM e a Susep.