RHE

SWEDEN DATA LEAK

never store sensitive data in a public cloud

Florian Postic

Sources :
https://korben.info/suede-balance-nature-donnees-personnelles-de-millions-de-citoyens.html
https://thehackernews.com/2017/07/sweden-data-breach.html

Never store sensitive data in cloud !

2015 : l’Agence Suédoise de Transport externalise ses données chez IBM.

Cette base contient des informations sur des millions de citoyens suédois ainsi que des secrets nationaux !

Il existe une pratique qui consiste à fournir ces données à des organisation marketing. Seulement l’envoi de ces données s’est fait en clair avec la base entière non nettoyé des données confidentielles.

Qu’est-ce qu’il y a exactement dans cette base de données ?

1. Les limites de poids de toutes les routes et ponts de Suède
2. Les noms, photos et adresses des pilotes de l’armée de l’air
3. Les noms photo et adresses des personnes enregistrés dans les fichiers de police
4. Les noms, photos et adresses de membre de l’unité d’élite commando
5. Les noms, photos et adresses d’origine de toutes les personnes qui ont changé d’identité via le programme de protection des témoins
6. Type, modèle, poids et défaillances de tous les véhicules gouvernementaux et militaires

OUI CA CRAINT !

Et c’est pas tout ...

De employés d’IBM hors de la Suède avaient tous les accès sur les logs et données contenus dans cette base.

Les services secrets suédois n’ont découvert cette fuite qu’en 2016.

Le directeur de l’agence a été viré en Janvier 2017 et a dû payer une amende de 70 000 couronnes suédoises (8500 $) pour "négligence dans le traitement de données secrètes"

Morale de l’histoire :

1. On n’externalise <u>jamais</u> des données sensibles dans le cloud.
2. Lorsque l’on transmet des données sensible on s’assure qu’elles soient correctement chiffrées.
3. Ne pas mélanger dans une seule base de données, des données de niveaux de sensibilité différents.
4. On limite au maximum le nombre d’utilisateurs ayant accès aux base de données sensibles et on s’assure que le principe du *need-to-know* et du *least privilege* soient respectés.