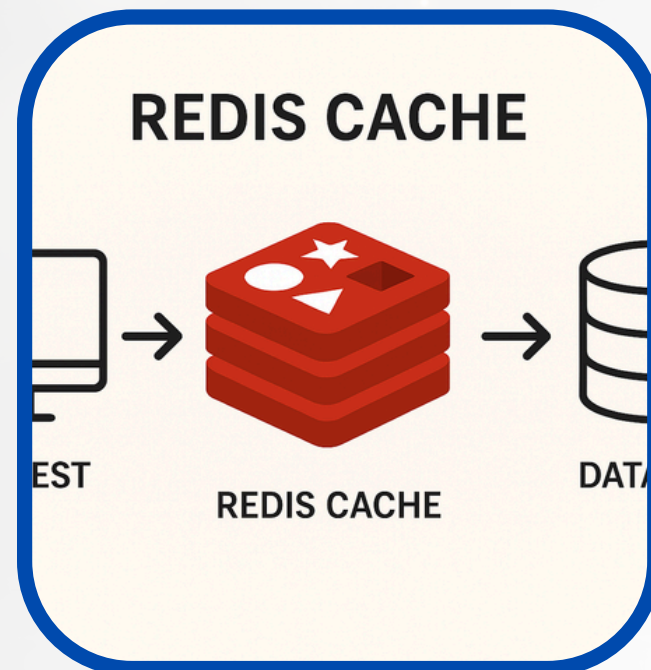


INCIDENT CHATGPT MARS 2023 : ANALYSE ET LEÇONS

Le 20 mars 2023, OpenAI (l'entreprise qui a créé ChatGPT) a désactivé temporairement ChatGPT pendant plusieurs heures, à cause d'un bug informatique.

Quelques utilisateurs avaient remarqué quelque chose d'étrange : Quand ils ouvraient ChatGPT, ils voyaient des informations personnelles d'autres utilisateurs s'afficher dans leur compte. dans certains cas, les utilisateurs ont aussi vu le titre de conversations d'autres personnes. Ce n'était pas un piratage, mais un bug technique dans un logiciel que ChatGPT utilisait pour fonctionner.





ChatGPT utilise un outil appelé Redis, un programme open-source (gratuit et public), pour stocker temporairement des données pendant qu'un utilisateur est connecté. C'est un système de cache : il garde en mémoire des informations utiles pour accélérer les réponses.



Pour faire fonctionner Redis avec le langage Python, OpenAI utilisait une bibliothèque appelée redis-py, également open-source. Le problème venait de redis-py. Ce logiciel avait un bug de gestion de mémoire : Quand plusieurs utilisateurs se connectaient en même temps, les “tampons” (zones mémoire qui gardent temporairement les données d’un utilisateur) pouvaient se mélanger. Résultat : un utilisateur pouvait recevoir les données d’un autre.



Cet incident illustre la vulnérabilité structurelle des systèmes numériques, y compris ceux gérés par des entreprises disposant de ressources considérables. Il met en lumière les risques spécifiques aux plateformes d'IA conversationnelle, qui manipulent des données potentiellement sensibles (informations personnelles, opinions, données professionnelles).





Bien que la fuite ait été limitée et rapidement corrigée, elle soulève des questions juridiques fondamentales liées à la protection des données personnelles et à la sécurité des traitements.



Dans cette affaire, il n'y a pas eu de recours ,
pourtant une action en responsabilité civile reste
possible .





Les principes de licéité, loyauté, transparence et de sécurité obligent le responsable du traitement à mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

