TD du thème 4

Valentin Massat-Seiller
Anthony Afonso

03/03/25

Mme Guelinel

SOMMAIRE

1. Dans cette procédure d'archivage, on peut considérer que la confidentialité des archives n'est pas garantie, parce que les personnes ayant acheté un serveur on accès a toute la salle des archives et donc toutes les archives. Mais également le fait que les données ne soient pas chiffrées, apporte une faille supplémentaire dans le SI. On peut noter, dernièrement, que l'utilisation d'une clé peut-être dangereuse par rapport à un fichier contaminé par un virus ou un autre type de malware, ce qui est, selon moi une faille majeur par rapport à cette situation.

2. On remarque tout d'abord que la pépinière ne possède qu'un serveur pour toutes les archives de toutes les startups présentent en son sein.

   Cette première information nous montre déjà qu'un dysfonctionnement quel qu'il soit du serveur d'archivage des données va bloquer toute rentrée d'archive. Et peut donc créer une insécurité des données, et une fuite potentielle peut-être envisageable.

3. L'entreprise Cibeco est considérée comme non-RGPD dû au faille présente dans le processus de conservation des archives mis en place par la pépinière. Ces failles sont à hauteur de 3 et empêchent la sécurité totale des données des clients. Notamment l'utilisation de la clé USB qui peut apporter au serveur un ou plusieurs logiciels malveillants dû à une inattention. On peut également retenir que les entreprises présentent dans la pépinière on accès aux archives de toutes les autres entreprises. Et pour conclure des données non chiffrées ne garantissent aucune sécurité dans le cas ou les différents niveaux de sécurité pour accéder à ces dernières soient outrepassé.

4. Premier cas : Une personne malveillante accède frauduleusement aux données archivées.
   - Dans ce premier cas, nous pouvons considérer que le niveau de gravité est important parce que la personne a accès aux données mais n'a pour le moment rien fait. Elle pourrait potentiellement récupérer des informations personnelles des

clients. Si l’on a conscience du problème, l’entreprise peut prévenir ses clients concernant les démarches à mettre en place.

Deuxième cas : Une personne malveillante modifie frauduleusement le contenu des données archivées.

- Pour ce deuxième cas, on peut considérer le niveau de gravité comme maximal, parce qu’une personne ayant modifié les données a pu tout d’abord les voir, puis faussé ces dernières. Cela ne garantit plus l’intégrité des données en plus de leur confidentialité.