Tamda Zohir
BTS Services Informatiques aux Organisations
Bloc 3 - Cybersécurité

Le 29 janvier 2024

Caractériser les risques liés à une utilisation malveillante du SI

Sommaire

Confidentialité des données non garanties

La confidentialité des données n’est pas garantie par la procédure d’archivage car elles ne sont pas chiffrées, ce qui fait que n’importe qui peuvent accéder aux données personnelles.

Également, l’entreprise Cibeco ne possède qu’un seul serveur, ce qui peut poser problème sur la disponibilité des services. Autre problème, Madame Darmon (responsable de l’entreprise Cibeco), archive manuellement les données tous les jours à 18:00 alors qu’il fallait effectuer cette tâche de manière automatique. Aussi, les clients qui ont loué un serveur dédié peuvent accéder à la salle de serveurs et prendre en compte le digicode alors qu’il faudrait ne pas faire confiance à eux.

Risque lié à l’indisponibilité du serveur d’archivage

Le serveur d’archivage peut mener au risque lié à l’indisponibilité du serveur d’archivage. En effet, les données qui ne sont pas chiffrées a pour conséquence de les rendre visibles pour tout le monde en cas de faille de sécurité.

Le premier risque est la capacité de stockage, en effet elle n’est pas suffisante pour archiver les données des clients, ce qui fait qu’on serait obligé de supprimer les fichiers d’archivage qui ne paraissent pas nécessaires alors qu’il n’est pas recommandé d’effectuer ce procédure. Pour faire face à ce problème, il est nécessaire d’augmenter la capacité de stockage en ajoutant plus de disques durs sur un autre serveur, qui a pour rôle d’archiver plus de données.

Le deuxième risque est le fait de se connecter avec un login et un mot de passe. Or, cette méthode d'authentification est vulnérable car une personne mal intentionnée peut utiliser des méthodes d’attaques permettant d’accéder au serveur et ainsi voler les données des clients. La solution face à ce problème est d’utiliser d’autres méthodes d'authentification plus sûres. Par exemple, on peut avoir la possibilité de se connecter au serveur avec une clé publique et clé privée, ou bien se connecter avec une passphrase (phrase de passe).

Enfin, autre problème, c’est que les archives ne sont conservées que durant 2 ans, passé ce délai, les données seront formatées et ainsi de suite. Pour éviter ce genre de risque, il est recommandé de ne pas les formater mais les supprimer à la demande des clients.

Politique d’archivage non conforme au RGPD

La politique d’archivage de l’entreprise Cibeco n’est pas conforme au RGPD car les informations sensibles (à savoir les transactions bancaires des clients) ne sont pas chiffrées et il se peut que Madame Darmon puisse voir ces informations durant le transfert de données d’archivage. Même si cela est fait de manière intentionnelle, on ne doit jamais voir les informations personnelles des clients. Aussi, comme les attaquants récupèrent les fichiers d’archivage, cela expose ces informations sensibles.

Pour connaître le niveau de risques des attaques, on peut utiliser un gestionnaire de gestion des incidents tels que GLPI dans lequel quelques informations vont être ajoutées tels que la date de l’incident, le niveau de gravité ainsi que la description.

Risque 1:

Ticket de déclaration d’un incident	
Date de l’incident: 01/02/2024 Niveau de gravité: ☐ Négligeable ☐ Limité ☐ Important ☑ Maximal	Description: Une personne malveillante accède frauduleusement aux données archivées.

Risque 2:

Ticket de déclaration d’un incident	
Date de l’incident: 02/02/2024 Niveau de gravité: ☐ Négligeable ☐ Limité ☐ Important ☑ Maximal	Description: Une personne malveillante modifie frauduleusement le contenu des données archivées.

Évaluation des risques

Le niveau de gravité défini pour le risque 1 est au niveau maximal (*très critique*) car l'attaquant peut voir les informations sensibles telles que les informations bancaires des clients. Par conséquent, il s'agit d'une fraude.

Enfin, le niveau de gravité défini pour le risque 2 est également au niveau maximal (*très critique*) car l'attaquant falsifie les informations, ce qui fait qu'il est impossible de connaître les transactions avec les clients, les données comptables et financières ainsi que les trafics réseau.