- HAFAIDH Mohamed
- HUYNH Jacky

BTS SIO1 - Gp1
BLOC 3 - Cybersécurité

THÈME 4

Caractériser les risques liés à une utilisation malveillante d'un SI.

Le 05/02/2024

Sommaire :

EXERCICE 1 :

Indiquez pourquoi la confidentialité des données archivées n'est pas garantie par la procédure d'archivage utilisée par Cibeco.

La notion de confidentialité repose sur le fait qu'une donnée n'est accessible qu'à ou aux personne(s) concernée(s).

La confidentialité des données archivées n'est pas garantie par la procédure d'archivage utilisée par Cibeco.

En effet, ces données sont, certes, stockées dans une salle possédant des serveurs protégés par un digicode, néanmoins tous les clients de Sarah DARMON et Sarah elle-même ont connaissance du digicode. Ainsi, il est possible que les données soient consultées (de manière volontaire ou non) par des clients non légitimes.

Également, Cibeco copie régulièrement les données à archiver sur une clé USB. Le souci étant que les données archivées ne sont pas chiffrées. En cybersécurité, l'élément ayant le plus de vulnérabilité est l'être humain, il est donc probable que la clé soit perdue par exemple et donc que la confidentialité ne soit plus garantie.

EXERCICE 2 :

Argumentez sur le risque lié à l'indisponibilité du serveur d'archivage de Cibeco compte tenu de la procédure d'archivage mise en place par l'entreprise.

L'indisponibilité du serveur d'archivage de Cibeco représente un risque majeur pour l'entreprise, car elle pourrait entraîner la perte ou la corruption des données archivées. Ces données comprennent des informations sensibles, telles que des données personnelles, des données financières et des données commerciales.

La procédure d'archivage mise en place par Cibeco présente plusieurs faiblesses qui augmentent le risque d'indisponibilité du serveur d'archivage :

- Le serveur d'archivage est un seul point de défaillance. En cas de panne du serveur, toutes les données archivées sont perdues.
- Le transfert des données vers le serveur d'archivage est réalisé manuellement, par la responsable de Cibeco. Cette opération est susceptible d'être source d'erreurs.
- Les données archivées ne sont pas chiffrées. Cela les rend vulnérables aux attaques malveillantes.

En cas d'indisponibilité du serveur d'archivage, Cibeco pourrait subir les conséquences suivantes :

Perte de données sensibles.

Les données personnelles, financières et commerciales pourraient être perdues ou compromises.

Cela pourrait entraîner des sanctions administratives ou pénales, ainsi que des dommages financiers pour Cibeco et ses clients.

Interruption de service.

La perte de données pourrait entraîner l'interruption de certains services fournis par Cibeco, tels que l'application web d'Ecotri.

Cela pourrait nuire à la réputation de l'entreprise et à ses relations avec ses clients.

Pour réduire le risque d'indisponibilité du serveur d'archivage, Cibeco doit mettre en place les mesures suivantes :

Déployer un second serveur d'archivage. Cela permettra de garantir la disponibilité des données en cas de panne du premier serveur.

- Automatiser le transfert des données vers le serveur d'archivage.
- Cela permettra de réduire le risque d'erreurs humaines.
- Chiffrer les données archivées.

Cela les rendra plus difficiles à déchiffrer par des attaquants malveillants.

Ces mesures permettront à Cibeco de réduire significativement le risque lié à l'indisponibilité du serveur d'archivage.

EXERCICE 3

Expliquez pourquoi la politique d'archivage de Cibeco n'est pas conforme au RGPD.

Non-conformité de la politique d'archivage de Cibeco au RGPD

Plusieurs manquements au RGPD sont présents dans la politique d'archivage de Cibeco, les rendant non conformes au règlement :

1. Manque de sécurité des données archivées :

- Absence de chiffrement : Les données archivées sur le serveur ne sont pas chiffrées, ce qui les rend vulnérables en cas de vol ou d'accès non autorisé au serveur.

- Transfert via clé USB : Le transfert des données à archiver via une clé USB présente un risque de perte ou de vol de la clé, exposant les données sensibles.

- Accès non contrôlé : Seul un mot de passe protège l'accès au serveur d'archivage, sans authentification multifacteur ni limitation des accès aux utilisateurs ayant un besoin légitime.

2. Conservation excessive des données :

- Durée de conservation non justifiée : La politique actuelle prévoit une conservation de 2 ans pour toutes les archives, sans distinction selon leur nature ou leur utilité.

3. Manque de transparence et de contrôle des personnes concernées :

- Absence d'information : Les clients ne sont pas informés de la nature des données archivées, ni de la durée de conservation.

- Absence de droit d'accès et de suppression : Les clients ne disposent d'aucun moyen d'accéder aux données archivées les concernant ou de demander leur suppression.

En résumé, la politique d'archivage de Cibeco expose les données sensibles à des risques de sécurité importants et ne respecte pas les droits des personnes concernées.

Risques et classification :

Risque 1 : Accès frauduleux aux données archivées

- Conséquences potentielles : Vol de données sensibles, usurpation d'identité, atteinte à la vie privée, préjudice financier.

- Niveau de risque : Élevé

Risque 2 : Modification frauduleuse du contenu des données archivées

- Conséquences potentielles : Corruption de données, falsification de documents, perte de preuves, altération de l'image de l'entreprise.

- Niveau de risque : Élevé

Recommandations :

- Mettre en place des mesures de sécurité techniques et organisationnelles pour protéger les données archivées (chiffrement, authentification forte, contrôle des accès).

- Définir une politique de conservation des données claires, simples et transparentes, en fonction de la nature et de l'utilité des données.

- Informer les clients des données archivées les concernant et de leurs droits (accès, rectification, suppression, etc…).

- Mettre en place une procédure de gestion des incidents pour détecter et répondre rapidement aux incidents de sécurité.

En conclusion, la politique d'archivage de Cibeco doit être révisée de manière urgente pour la mettre en conformité avec le RGPD et garantir une sécurité des données sensibles.

Note : Le document "Extrait du ticket de déclaration d'un incident" n'est pas exploitable pour répondre à la question car il ne contient aucune information relative aux risques identifiés ou à la procédure de classification.

EXERCICE 4

Justifiez, pour chacun des risques, le niveau de gravité à sélectionner dans la liste déroulante du ticket de déclaration d'un incident.

Le niveau de gravité pour qu'une personne malveillante accède frauduleusement aux données archivées peut être considéré comme important.

En effet, le principe de confidentialité n'est pas respecté, la consultation de ces données par une personne malveillante peut entraîner une fuite de données sensibles ainsi que l'accès au données personnel du client.

Par exemple, si une personne malveillante accède frauduleusement à des données archivées, elle peut les communiquer à d'autres personnes qui eux pourraient les communiquer à d'autres également. Cet effet papillon a donc de lourdes conséquences ou ils peuvent être revendus sur le web.

Également, le niveau de gravité pour qu'une personne malveillante modifie frauduleusement le contenu des données archivées peut être considéré comme maximal.

En effet, modifier une donnée archivée relève d'une rupture du principe d'intégrité. Une personne malveillante modifiant ces données les rend totalement falsifiées. D'autant plus, que la modification entraîne forcément une consultation.

Ainsi, cette personne peut en premier lieu consulter, les communiquer à d'autres personnes non légitimes, mais également elle peut les modifier les rendant totalement fausses et non intègres.