ZIZA KANGUE SARAH

I)Caractériser les risques Liés à une utilisation malveillante d'un système informatique.

1. La confidentialité des données archivées par Cibeco ne peut être garantie pour plusieurs raisons :

-Les données archivées ne sont pas chiffrée. Cela signifie que si quelqu'un parvient à accéder aux données, il peut les lire sans aucune restriction.

-Transfert de données via une clé USB librement accessible. Cela crée des risques car la clé USB peut être perdue, volée ou utilisée par des personnes non autorisées.

2. Les risques liés à l'indisponibilité du serveur d'archives Cibeco sont également importants :

-Il n'y a qu'un seul serveur pour tous les fichiers. Si ce serveur tombe en panne, toutes les données archivées seront inaccessibles jusqu'à ce que le serveur soit réparé.

- Le processus d'archivage est effectué manuellement tous les jours à 18h00. Si ce processus est interrompu pour une raison quelconque, les données de cette journée ne seront pas archivées.

3.La politique d'archivage de Cibeco pourrait ne pas être conforme au RGPD pour plusieurs raisons :

- **Consentement des Utilisateurs** : Le RGPD exige que le consentement pour le traitement des données personnelles soit donné de manière libre, spécifique, éclairée et univoque.
- **Sécurité des Données** : Les entreprises doivent mettre en place des mesures techniques et organisationnelles appropriées pour protéger les données contre la perte, l'altération ou l'accès non autorisé dans le cas de ciberco la sécurité des données n'est pas respecter.
- **Droits des Sujets de Données** : Les individus ont le droit d'accéder à leurs données, de les rectifier, de les effacer, et de s'opposer à leur traitement.

4.

Afin d'évaluer la gravité de chaque risque, il faut tenir compte de l'impact potentiel sur l'entreprise si le risque se réalise.

Risque 1 : Une personne malveillante accède frauduleusement aux données archivées.

Ce risque peut être classé comme risque maximum. Si les attaquants accèdent aux données archivées, ils pourraient accéder à des informations sensibles telles que les transactions clients, les données comptables et financières, ainsi que les données liées au trafic réseau des clients. Cela peut entraîner des violations de la confidentialité des données avec de graves conséquences juridiques et financières pour l'entreprise.

Risque 2 : Une personne malveillante modifie frauduleusement le contenu des données archivées

Ce risque peut également être classé comme risque maximum. Si le contenu des données archivées est modifié, l'intégrité des données de l'entreprise peut être affectée. Par exemple, si les données financières changent, cela pourrait fausser les informations financières d'une entreprise, avec des conséquences juridiques et financières.

II) Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité.

1)les conséquences techniques de l’attaque subie par Ecotri

Intégrité : le site a été défacer .

Disponibilité : le site n’est pas accessible.

Confidentialité : les données personnelles des membres d’ecotri sont afficher publiquement sur le site.

2)les développeurs de cibeco on laisser un exemple de code produit d’où le formulaire peut être modifier ou des données peuvent être insérer donc compromettre la question d’intégrité.

3)les conséquences de ecotri cette attaque sont les suivantes :

Humaines : Impacts sur la sécurité ou sur la santé des personnes :

Parmi les données qui ont été publiée il y’à l’adresse la sécurité des membres peut être compromise ils pourront subir par la suite des vols.

Financière : conséquences pécuniaires :la crédibilité de ecotri prendra un coup donc ont à une baisse financière importante du au retrait de certains client.

4) Les conséquences juridiques auxquelles les agresseurs sont confrontés sont :

Sanctions pénales : les attaquants peuvent être poursuivis pour diverses infractions liées à la cybercriminalité, telles que l'accès frauduleux à des systèmes informatiques, l'endommagement d'ordinateurs ou la violation des lois sur la protection des données personnelles lorsque des informations sensibles sont compromises.

Responsabilité Civile : L'attaquant pourra être tenu responsable des dommages causés au site Ecotri, notamment des pertes financières, de l'interruption des activités commerciales ou de la réputation.

Mesures correctives : outre les sanctions pénales et les dommages financiers, les attaquants peuvent être contraints de prendre des mesures correctives, telles que la restauration des données, la mise en œuvre de mesures de sécurité renforcées ou des excuses publiques.

Quant à l'identification de l'adresse IP de l'attaquant, oui, dans la document5, l'adresse IP de l'attaquant semble être identifiée comme « 82.89.34.7 ».