Rapport Projet :   
TechnoGroupMedical

**Exercice 1 : Proposer une architecture réseau sécurisée qui assure une communication sécurisée entre les différents sites dans les quatre coins du pays.**

* Pour sécuriser la communication entre les différents sites de notre entreprise, nous allons utiliser un réseau combinant FTP (File Transfer Protocol) et VPN (Virtual Private Network). Le FTP est un protocole de transfert de fichiers qui permet de transférer des fichiers entre des ordinateurs sur un réseau. Il est fiable et efficace pour le transfert de grandes quantités de données, tout en garantissant la confidentialité des données transmises grâce à une cryptographie de niveau supérieur.

Le VPN, quant à lui, permet de créer une connexion sécurisée entre des réseaux distants. Il permet de créer une connexion privée virtuelle entre les différents sites, permettant ainsi d'échanger des données de manière confidentielle et sécurisée. En utilisant le VPN, nous pouvons également nous assurer que les données transmises ne sont pas altérées ou modifiées en transit.

En combinant ces deux technologies, nous pouvons garantir la confidentialité et l'intégrité des données transmises entre les différents sites, ce qui est essentiel pour protéger les données sensibles de notre entreprise.

* Pour mettre en œuvre cette solution de sécurité du réseau, nous devons suivre les étapes suivantes :

Configuration du VPN : Nous devons configurer le VPN pour établir une connexion sécurisée entre les différents sites. Cela implique de

définir les paramètres de cryptage et d'authentification, ainsi que les protocoles utilisés pour la communication.

Configuration du FTP : Nous devons également configurer le FTP pour permettre le transfert sécurisé de fichiers entre les différents sites. Cela implique de définir les autorisations d'accès et les répertoires de stockage.

Mise en place de contrôles d'accès : Pour renforcer la sécurité, nous devons également mettre en place des contrôles d'accès pour les différents équipements et applications utilisées dans le réseau. Cela peut inclure l'utilisation de mots de passe forts, de pare-feu et d'autres mesures de sécurité.

En suivant ces étapes, nous pouvons garantir la mise en œuvre réussie d'une solution de sécurité du réseau qui assure une communication sécurisée entre les différents sites de notre entreprise.

Les sites :

A picture containing text

Description automatically generated

Dans cet exemple on veut transférer les fichiers du pc de Phil au FTP Private

Diagram

Description automatically generated

Diagram

Description automatically generated

On Connecte le VPN

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Puis on envoie le Fichier Encrypter au FTP privée

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

**Exercice 2 :** **Proposer des contrôles d’accès qui protégeront votre technologie (un appareil qui révolutionne la médecine).**

Pour protéger notre technologie révolutionnaire, nous allons mettre en place des contrôles d'accès rigoureux. Ceux-ci comprennent :

* Authentification forte : Nous allons utiliser des méthodes d'authentification robustes, telles que les mots de passe uniques et sécurisés avec des politiques de complexité de mots de passe pour garantir la sécurité des comptes d'utilisateurs.
* Autorisation : Nous allons définir les rôles et les autorisations en fonction des besoins d'accès à la technologie pour garantir que les informations sensibles ne soient accessibles qu'aux personnes autorisées.
* Contrôles de session : Nous allons mettre en place des contrôles de session pour garantir que les sessions soient automatiquement déconnectées après un certain temps d'inactivité et que les informations sensibles soient protégées.

Pour renforcer la sécurité, nous allons également mettre en place les contrôles d'accès supplémentaires suivants :

* Journalisation des activités : Nous allons enregistrer les activités des utilisateurs sur la technologie pour pouvoir les examiner en

cas de besoin et pour détecter les tentatives d'accès non autorisées.

* Cryptage des données : Nous allons crypter les données sensibles pour garantir leur confidentialité et leur intégrité pendant leur transfert et leur stockage.
* Mise à jour de sécurité régulière : Nous allons maintenir la technologie à jour avec les dernières mises à jour de sécurité pour garantir sa protection contre les menaces informatiques émergentes.

En mettant en place ces contrôles d'accès rigoureux, nous pouvons garantir la sécurité de notre technologie révolutionnaire.

**Exercice 3 :** **Proposer une solution qui assure la disponibilité du serveur fichier qui se trouve dans un datacenter au sous-sol l’immeuble.**

Donc pour garantir la disponibilité du serveur de fichiers, nous proposons de mettre en place des solutions de sauvegarde et de récupération de données pour minimiser les temps d'indisponibilité en cas de panne. Nous recommandons également d'utiliser des technologies de virtualisation pour garantir la continuité des opérations en cas de défaillance matérielle.

**Exercice 4 : Motiver votre demande de renouvellement en expliquant la menace, le risque et l’impact.**

Mesdames, Messieurs,

Je vous écris pour exprimer mon souhait de renouveler le certificat d'authentification pour le site web de notre entreprise. Comme vous le savez, notre entreprise a fait l'acquisition d'une nouvelle technologie révolutionnaire qui nous distingue sur le marché et nous permet de répondre à la forte demande de soins. Cependant, pour assurer la sécurité de notre site web et protéger notre technologie innovante, il est important que nous maintenions un niveau élevé de sécurité en ligne.

Le certificat d'authentification est un élément crucial pour la sécurité de notre site web. Il garantit à nos utilisateurs que le site web qu'ils visitent est bien celui de notre entreprise et non pas une imitation malveillante. En cas de non-renouvellement du certificat d'authentification, notre entreprise sera exposée à diverses menaces telles que le phishing et les attaques de type Man-in-the-Middle. Si un utilisateur tombe sur un site web malveillant en pensant qu'il s'agit du site web de notre entreprise, il pourrait partager des informations sensibles telles que des informations de carte de crédit ou des informations personnelles.

Cela pourrait entraîner une perte de confiance de la part de nos utilisateurs et de nos clients potentiels, ce qui pourrait avoir un impact négatif sur les ventes et la réputation de notre entreprise. De plus, le manque de protection de nos informations confidentielles pourrait entrainer des violations de la confidentialité des données de nos clients, ce qui pourrait entraîner des conséquences juridiques graves pour notre entreprise.

Je vous prie de prendre en considération ma demande de renouvellement du certificat d'authentification pour le site web de notre entreprise. Je suis persuadé que ce petit investissement assurera la protection de notre technologie innovante et garantira la sécurité de nos utilisateurs et de nos clients. Je suis prêt à discuter de la situation en détail lors d'une réunion à votre convenance

Je vous remercie de l'attention que vous porterez à ma demande.

Cordialement

Responsable de la sécurité des systèmes d'information

**Exercice 5 :** **Quelles sont les mesures que vous avez mises en place pour être en conformité avec le RGPD?**

En tant que responsable de la sécurité des systèmes d'information pour votre entreprise qui collecte des données à caractère personnel, nous avons mis en place les mesures suivantes pour garantir la conformité avec le Règlement général sur la protection des données (RGPD) :

-Mise en place de politiques de sécurité des données strictes pour garantir la confidentialité et la sécurité des informations.

-Formation des employés sur les bonnes pratiques de protection des données personnelles.

-Mise en place de contrôles d'accès stricts pour les données sensibles pour minimiser les risques de fuite de données.

-Utilisation de technologies de chiffrement pour protéger les informations en transit et en stockage.

-Mise en place de processus de gestion des incidents de sécurité pour gérer les brèches éventuelles.

-Collaboration avec des auditeurs indépendants pour s'assurer de la conformité RGPD.

Ces mesures garantissent la protection des données à caractère personnel et la conformité avec les exigences du RGPD.