ENSEEIHT 3A SN-L 2021-2022
Partiel sécurité

Durée 1h30
Sans documents

Note

Afin de simplifier le sujet du partiel, beaucoup de détails techniques sont ignorés. Si vous faites des suppositions ou hypothèses quant à ce qui existe sur le système cible, *indiquez-les clairement*.

Note

Vous allez faire une analyse de risques (simplifiée). Il est **particulièrement important** que vous argumentiez vos choix.

1. Contexte

La société C&T intervient dans le domaine très compétitif des véhicules n'utilisant pas d'énergie fossile. Elle est spécialisée dans la recherche de nouveaux moyens de propulsion, dont les piles à hydrogène et les moteurs électriques. Son personnel (150 collaborateurs) est réparti en deux grandes populations : des chercheurs (60 personnes) et des spécialistes de l'industrialisation (50 personnes). Les autres collaborateurs constituent l'équipe nécessaire pour la gestion de l'entreprise (comptabilité, finances, ressources humaines, etc.).

Les bâtiments qui hébergent les équipes de recherche sont implantés dans une zone rurale. Ils sont loués à une municipalité, qui a mis en place une infrastructure spécifique afin d'accueillir des activités non industrielles. Deux bâtiments utilisés par les équipes d'industrialisation sont implantés en périphérie d'une grande ville, dans les locaux d'une ancienne usine rachetés par C&T. Enfin, le siège social est implanté dans le centre de la même ville près de laquelle se trouvent les équipes d'industrialisation, dans un bâtiment appartenant aussi à l'entreprise.

2. Description du système d'informations

L'illustration 1 présente schématiquement l'organisation informatique de C&T.

Chaque site dispose d'une connection à Internet. Cette connexion est mise en œuvre par des équipements spécifiques (arrivée fibre optique et routeur séparé) achetés par C&T. Les sites sont interconnectés, par le biais de boîtiers VPN chiffrants.

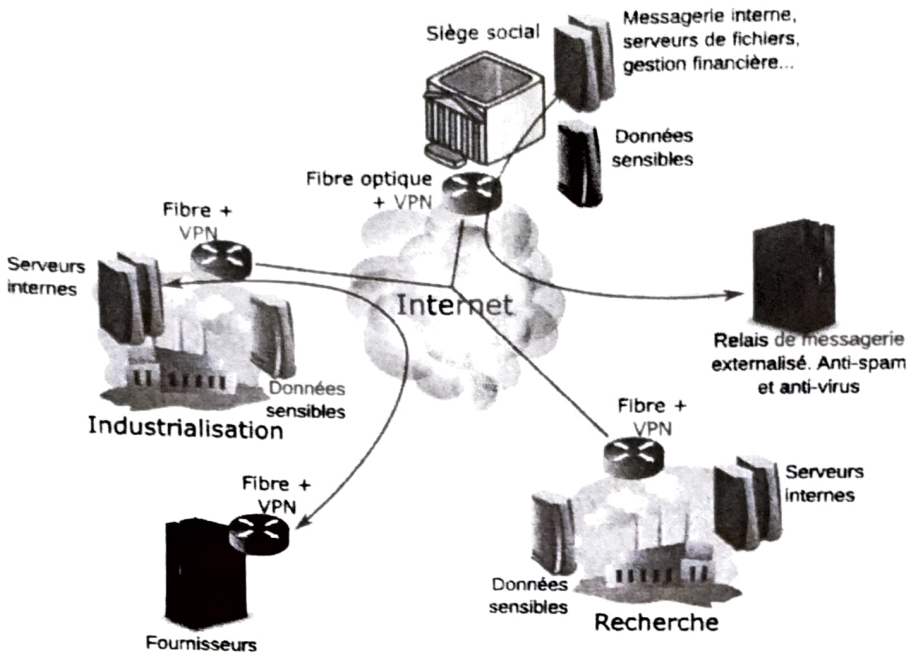

ILLUSTRATION 1 : Organisation générale du SI de C&T

La navigation vers Internet est libre depuis chaque site. La messagerie est partiellement externalisée chez un prestataire, qui reçoit tous les messages (envoyés ou destinés à C&T) et procède à leur acheminement. Ce prestataire fait relais anti-spam et anti-virus, essentiellement pour les courriels entrants. Les boîtes à lettres des collaborateurs de C&T sont gérées par l'entreprise sur un serveur spécialisé situé au siège social.

Les sites disposent de leurs propres serveurs de données. Les données sensibles (au sens industriel) des sites de recherche et d'industrialisation sont dupliquées tous les soirs vers un serveur du siège social. Lorsqu'un projet de recherche passe en phase de pré-industrialisation, les données associées sont transférées vers le site d'industrialisation, sur son serveur de données. Les données originelles sont archivées sur le site de recherche, sur des supports de stockage spécifiques qui ne sont mis en ligne qu'au moment de réaliser une archive.

Les sauvegardes sont réalisées sur chaque site, et dupliquées en temps réel (RAID au travers du réseau) vers un serveur sur le site du siège social. Pour ce dernier, les sauvegardes sont dupliquées vers le site de recherche.

Chaque site dispose d'une seule plage d'adresses :

— Le siège social utilise la plage `192.168.17.0/24`,
— le site de recherche utilise la plage `192.168.51.0/24`
— et le site d'industrialisation utilise la plage `192.168.84.0/24`.

Sur chaque site, les ordinateurs et serveurs sont reliés à des commutateurs, lesquel sont reliés au routeur.

Des fournisseurs (une trentaine d'entreprises situées en divers points du monde) peuvent se connecter, au travers d'un VPN, au site d'industrialisation. Ces fournisseurs vont chercher et déposer des informations spécifiques sur un serveur de fichiers mis à leur disposition par C&T. Il s'agit notamment de devis, plans de fabrication, schémas et autres informations techniques associés aux travaux menés par l'unité d'industrialisation.

Les boîtiers VPN utilisés (tant par C&T que par les fournisseurs) ont été achetés et

configurés par le service informatique de C&T. Ils sont tous configurés exactement de la même manière (à l'exception de leurs adresses IP).

Les postes de travail des sites de recherche et d'industrialisation utilisent GNU/Linux. Les postes de travail du siège social utilisent Windows 10. Tous les serveurs, sur chaque site, sont des machines fonctionnant sous GNU/Linux.

Des correspondants informatiques, sur les sites de recherche et d'industrialisation, gèrent les postes informatiques et le réseau.

3. Questions

Note

Nous supposons qu'il n'existe aucun élément de sécurisation qui ne serait pas décrit précédemment. Si, dans vos analyses et réponses, vous faites des hypothèses quant à ce qui existe ou devrait exister, signalez de façon explicite ces hypothèses. Afin de simplifier votre travail, nous considèrerons qu'il n'existe pas de contraintes budgétaires pour l'élaboration des solutions.

Note

Dans toutes les réponses, il est attendu que vous **justifiez** votre avis.

1. Indiquez les principaux risques que vous identifiez par rapport à l'organisation et au fonctionnement du système d'informations de C&T, en les classant par gravité décroissante. **Justifiez et argumentez** votre analyse.
2. Pour les trois principaux risques identifiés, discutez des mesures de prévention, de détection et/ou de contingentement que vous proposeriez à C&T. Discutez de leurs avantages et inconvénients.
3. C&T subi régulièrement des usurpations de comptes (hameçonnage/phishing, forçage de mots de passe) sur son réseau interne. Certaines de ces attaques ne sont détectées qu'apres des fuites de données industrielles sensibles. Quelles modifications/améliorations, techniques ou non, suggèreriez-vous pour limiter ou éviter ce genre d'incident ?
4. C&T veut limiter l'accès de ses partenaires au strict minimum nécessaire à chaque entreprise (ce « minimum » peut varier selon les partenaires). Que mettriez-vous en place pour atteindre cet objectif ? Quels sont les inconvénients (autres qu'une éventuelle complexification du système d'informations) associés à vos suggestions ?