N7 3AI 2017-2018
Partiel sécurité

Durée 2 heures

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*.

1. Contexte

La société CREUZE & TROUVE (C&T dans la suite du document) 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, les moteurs électriques et les combustibles novateurs. 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 trois bâtiments qui hébergent les équipes de recherche sont implantés dans une zone rurale. Ces bâtiments sont loués à une municipalité, qui a mis en place une infrastructure spécifique afin d'accueillir des activités non industrielles. Les deux bâtiments utilisés par les équipes d'industrialisation sont implantés en périphérie d'une grande ville, dans les locaux d'une ancienne usine achetés par l'entreprise. 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 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 (modem ADSL + routeur séparé) achetés par C&T. Les sites sont interconnectés, par le biais de boîtiers VPN chiffrants.

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 aussi relais anti-spam et anti-virus.

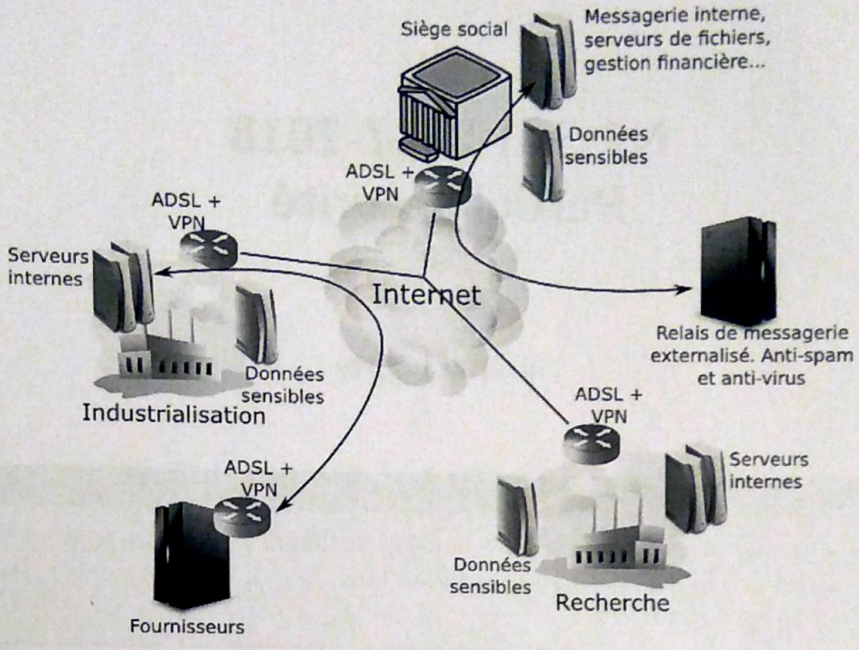

Illustration 1 : Organisation générale du SI de C&T

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 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 sensibles. Les données originelles sont archivées sur 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, tous les ordinateurs et serveurs sont reliés à un commutateur, sur lequel est aussi branché le boîtier ADSL/VPN.

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 Seven. 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. Question

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 signalant ce que vous considérez comme les trois principaux risques. 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 soupçonne l'un de ses fournisseurs de récupérer plus d'informations qu'il ne devrait. L'architecture actuellement en place permet-elle à C&T de confirmer ses soupçons ? Que proposeriez-vous à C&T pour un meilleur contrôle des actions de ses fournisseurs sur son réseau informatique ?
4. Des données de recherche de C&T ont été retrouvées chez un concurrent de l'entreprise. En supposant qu'il ne s'agit pas d'un collaborateur de C&T qui aurait transmis ces informations, que feriez-vous pour identifier l'origine de la fuite de données ? Pour éviter qu'un tel incident ne se reproduise ?