QUESTION 1 (40%)

L'entreprise LA MODE fait affaire au Canada depuis l'année 2000. Son siège social se trouve à Montréal où se trouve le centre des données globales de la compagnie. Elle est établie dans 15 villes canadiennes. Dans chacune de ces villes, elle possède 10 succursales. La communication entre les succursales et le siège social se fait à travers Internet. Également, l'entreprise effectue des ventes en ligne. L'infrastructure informatique de toutes les succursales est identique (Figure 1). Les réseaux physiques des succursales sont sans fil. Depuis la COVID, 50% des employés travaillent de la maison.

Les ingénieurs qu'elle a engagés pour développer le système ont proposé une architecture répartie basée sur le modèle client/serveur (Figure 1).

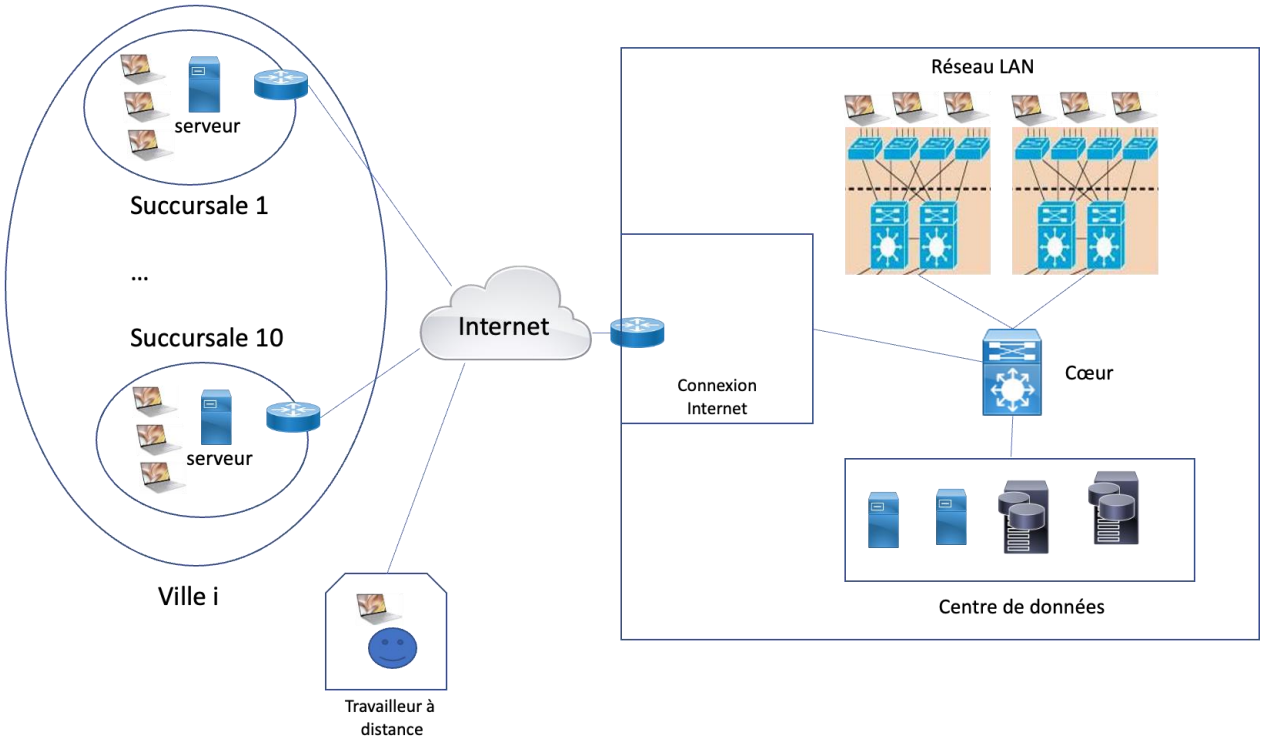


Figure 1. Répartition des succursales et du siège social de LA MODE.

Dans cette architecture, chaque succursale possède son propre serveur, cependant la base de données est centralisée et elle est localisée au centre de données du siège social.

L'architecture pour l'application, 3-tiers, de transactions en ligne est schématisée dans la figure 2. L'architecture de cette application est basée sur les notions de client/serveur (C/S).

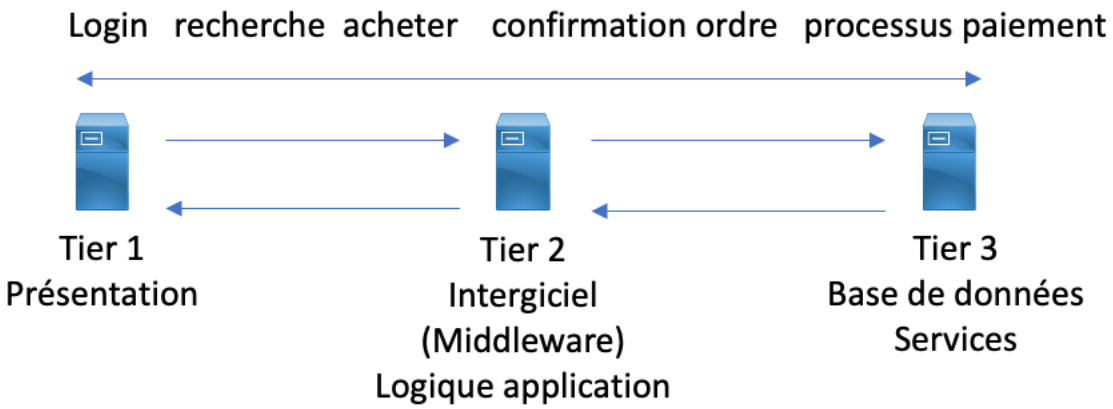


Figure 2 : Architecture de l'application client/serveur 3-tier.

Sachant que vous êtes des ingénieurs avisés en sécurité, **LA MODE** voudrait avoir votre avis sur certaines questions qu'elle se pose à propos de la sécurité du système réparti.

Vous devez proposer une architecture réseau détaillée qui tient compte de la sécurité pour chaque succursale, pour le siège social, le centre de données du siège social, pour la communication des travailleurs à distance, ainsi que pour le système réparti (pour les transactions en ligne) en tenant compte de l'approche défense en profondeur et des éléments de sécurité suivants :

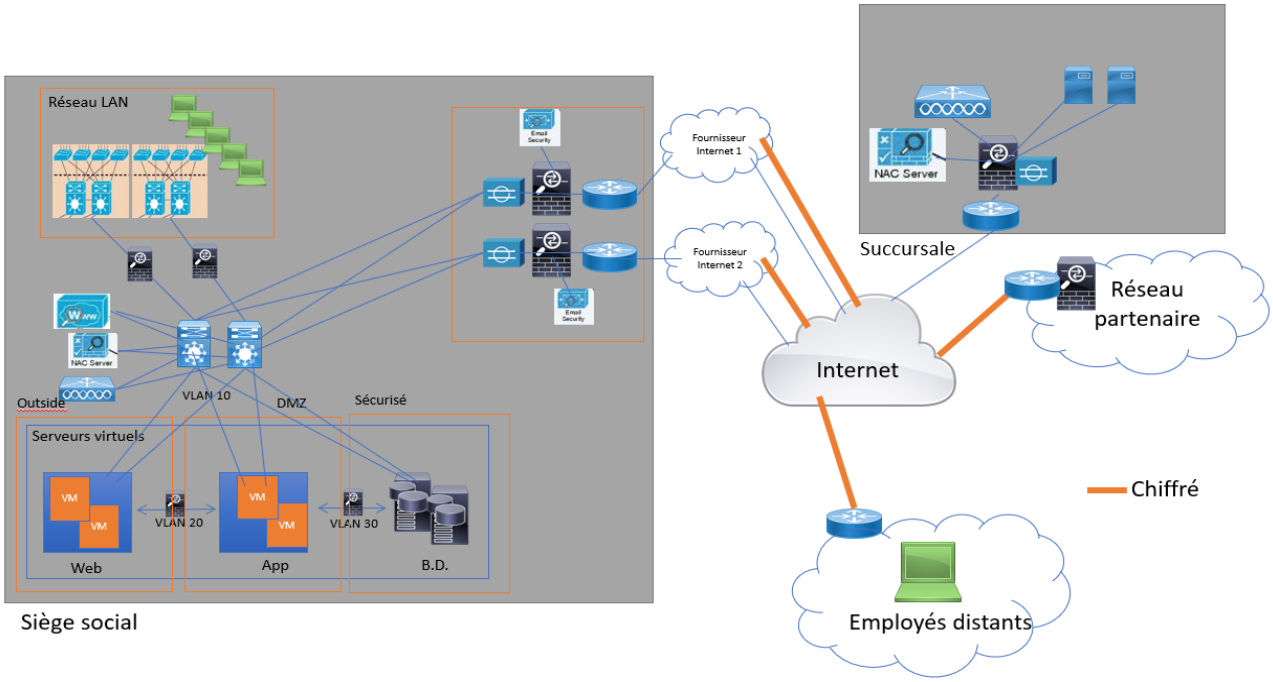
- L'architecture réseau des villes et du siège social sont 3-tiers.
- Définition des zones de sécurité.
- Dispositifs de contrôle d'accès.
- Mécanismes d'authentification.
- NAT.
- « Virtual private network » VPN.
- Fiabilité.
- Mobilité des utilisateurs.
- Redondance.
- Système de détection d'intrusion IDS ('Intrusion Detection System').
- Mécanisme d'authentification.
- Pare-feu (`firewall').
- Mécanismes de protection WiFi.
- Chaque succursale possède une connexion à Internet.
- Les succursales ont des réseaux sans fil.
- Les succursales permettent aux employés d'utiliser leurs dispositifs pour se connecter au réseau (BYOD : 'bring your own device').
- Montrer un schème avec l'analyse du trafic.

VOUS DEVEZ JUSTIFIER CLAIREMENT VOTRE ARCHITECTURE PROPOSÉE ET VOS CHOIX (dispositifs et protocoles utilisés).

Réponse

Globalement, l'entreprise communique à travers l'Internet avec ces différentes succursales, ces employés travaillant depuis la maison et également avec des réseaux de partenaires (processus de paiement par exemple).
Afin de sécuriser les communications entre siège et succursales il faudra s'assurer qu'à l'entrée de chacune des interfaces (bloc d'accès internet), il y ait un système de sécurité (pare-feu externe et IDS/IPS).
Entre le siège et les employés distants/les partenaires, il faudrait chiffrer les communications, en utilisant par exemple un VPN. Pour augmenter la sécurité des réseaux internes au sein de l'infrastructure, on utilisera des NATs (surtout que les réseaux des succursales sont non filaires).
Les succursales devront accéder à la base de donnée du siège car elles n'en ont pas localement. Pour sécurer cette communication on va chiffrer ces données aussi.
Pour implémenter l'architecture logiciel 3-tiers de l'application, on met en place des réseaux locaux virtuels que l'on sécurise avec des pare-feu virutels.
Pour assurer la mobilité des utilisateurs, nous aurons un réseau de points d'accès (routeur) réparti à travers les bâtiments de l'entreprise (siège et succursales). Pour les utilisateurs à distance, ils pourront accéder aux services de l'entreprise par l'intermédiaire du siège et des succursales (pas seulement du siège – qui pourrait représenter beaucoup de saut de nœuds réseaux donc du délai s'il est éloigné de l'utilisateur).
Pour assurer la résilience du réseau, nous avons une duplication de composants dans notre infrastructure.

Voici ci-dessous le schéma de l'architecture proposée pour l'entreprise LA MODE, incluant les dispositifs nécessaires pour assurer la sécurité.



QUESTION 2 (20%)

Pour les journalistes, un des aspects le plus important est la confidentialité/sécurité de leurs communications. Certains journalistes travaillent dans des zones à haut risque dans des dossiers très confidentiels, et pour d'autres qui travaillent dans le siège social du journal ces dossiers sont considérés très sensibles. Le directeur du journal a demandé au directeur du service informatique de fournir une solution pour la communication sécuritaire de ses journalistes, peu importe le site du travail (dans le réseau local ou à l'extérieur).

Le service informatique considère deux solutions possibles pour la communication : VPN et le réseau oignon (THOR). **Vous devez faire une comparaison de ces deux solutions proposées en considérant deux points de vue** :

- Les utilisateurs (journalistes) : quels sont les avantages et les inconvénients pour l'utilisation quotidienne de ces solutions afin de garantir une communication sécuritaire?
- Les responsables du service informatique qui doivent installer et entretenir l'infrastructure et les protocoles utilisés pour ces deux solutions. Quels sont les avantages et les inconvénients pour chacune de ces solutions : VPN et THOR?

Réponse

Point de vue des utilisateurs :
Pour les utilisateurs il y aurait plus d'avantages à implémenter une communication utilisant le VPN plutôt que THOR.
S'ils utilisent le réseau THOR, la performance sera grandement réduite comparée au VPN. THOR fait passer la communication par de multiples nœuds intermédiaires afin de bien protéger l'adresse IP de la source, cependant cela implique un délai significativement plus grand lors de chacune des requêtes. Pour le VPN on redirige le traffic à travers des hôtes (nœuds) spécifiques en tunnel. La sécurité de l'utilisateur est donc moindre comparée à celle ajoutée par THOR mais la performance est meilleure.
D'un point de vu utilisateur on préviligie l'expérience utilisateur, donc c'est mieux d'avoir un délai minimum, on choisierait donc le VPN.

Point de vue des responsables de l'infrastructure :
Pour le service informatique, cela sera plus avantageux en installation et en maintenance infrastructure de choisir le réseau oignon.
Afin que les utilisateurs aient des communications sécurisées avec THOR, il suffira d'installer et d'utiliser le navigateur web, il n'y a pas de configuration ou de maintenance en surplus à faire. Au contraire avec un service VPN interne, ce sera la responsabilité des employés du service informatique de configurer et de maintenir la communication pour qu'elle reste uniforme à travers le réseau local et surtout à l'extérieur peu importe le site de travail des journalistes. En effet, il faudra arriver à rigousement maintenir un politique VPN à travers l'entreprise au risque d'avoir des failles de sécurité.
Donc pour les responsables informatique c'est plus avantageux d'utiliser le réseau THOR car il y a moins de maintenance à faire, cela sera plus sécuritaire mais va causer des grands délais au niveau des communications.

QUESTION 3 (20%)

En 2018, 7 personnes de moins de 18 ans se sont fait voler leur identité, selon le Centre antifraude du Canada (CAFC). Ce nombre est passé à 13 en 2019 et à 175 en 2020. En 2021, les statistiques ont explosé : 1103 enfants et adolescents ont été victimes de vols d'identité, dont 93 % au Québec (La Presse, septembre 2022). Cette même tendance existe chez les adultes. Le nombre de vols d'identité a augmenté considérablement ces dernières années. Cette augmentation est due en partie à l'information « privée » (i.e. date de naissance, numéro de téléphone, adresse de domicile, etc.) qui est se trouve dans les réseaux sociaux.

Il est possible de collecter toute cette information ('Open Source Intelligence – OSINT' ou renseignements de sources ouvertes) grâce aux différents outils disponibles sur Internet qui cherchent des informations non classifiées qui ont été délibérément découvertes, discriminées, distillées et diffusées à un public choisi afin de répondre à une question spécifique. Par exemple, dans certains réseaux sociaux, les utilisateurs publient leurs dates de naissance et elles deviennent connues pour leurs contacts.

Comment faire pour diminuer ou réduire la collecte de données personnelles sur les réseaux sociaux afin d'éviter le vol d'identité? Justifiez clairement votre réponse.

Réponse

Afin de diminuer la collecte de données personnelles par les réseaux sociaux il est important de faire de la prévention par l'éducation à cette problématique. Il reste impossible d'éviter totalement tous les OSINT, mais si nous sommes conscient de cela, il sera possible de faire plus attention aux informations que l'on rend public, mais aussi de faire l'analyse des informations que nous devons garder public comme nom, prénom, éducation, emploie sur LinkedIn par exemple. Cela nous permet de mieux connaître nos potentiels points faibles.
Les principales actions à faire sont donc en lien avec la sensibilisation du public pour réduire le partage de ces informations – si inutiles, en ligne.
Il existe également une solution afin de contourner ce problème. Dans les services en ligne ou en présentiel d'identification, nous devrions soutenir et pousser l'identification à plusieurs facteurs. C'est-à-dire que pour assurer l'authenticité d'un individu, on demande par exemple, deux pièces d'identités différentes, ou encore on peut demander un identificateur comme l'empreinte d'un doigt et un mot de passe. De nos jours, beaucoup d'applications utilisent par exemple un code secondaire au mot de passe qui est envoyé à l'adresse courriel ou au cellulaire afin de compléter la connexion d'un individu.

QUESTION 4 (20%)

Une des présentations des étudiants est sur 'Facebook Phishing' ou 'Facebook Hameçonnage'. Dans la présentation, il est indiqué que : « L'un des vecteurs les plus courants de ce type de cyberattaque est de cibler les comptes Facebook et Google en envoyant un message ou un lien

suspect qui demande une information personnelle (comme un courriel, un numéro de téléphone ou un mot de passe).

Les attaquants ont tendance à créer de faux sites Web qui sont pratiquement identiques aux sites légitimes. Une fois que vous avez entré vos informations d'identification sur eux, ils les collectent et en tirent parti. »

Dans la même présentation, les étudiants ont indiqué certaines mesures préventives :

- Supprimez les courriels suspects.
- Utilisez des filtres anti-spam.
- Changez régulièrement les mots de passe des comptes et n'utilisez jamais le même mot de passe pour chaque compte.
- Évitez d'utiliser les réseaux publics lorsque vous accédez à des informations sensibles telles que des documents d'identification et des plateformes bancaires.
- S'il y a des liens hypertexte, passez la souris sur l'URL, le lien peut se diriger vers un site complètement différent. Faites attention à l'orthographe de l'URL, de petits changements dans un lien valide peuvent passer inaperçus. Exemple : « facebook.com » vs « fasebook.com ».
- Configurez les paramètres de navigation pour éviter l'ouverture de sites Web trompeurs.

Considérez un utilisateur qui ne comprend pas les aspects de sécurité informatique et qui n'a pas les notions basiques d'informatique (99% des utilisateurs d'Internet). **Vous devez analyser chacune de ces mesures pour ce type d'utilisateurs et dire quels sont les avantages et les inconvénients de ces mesures. Finalement, en utilisant vos réponses, expliquez pourquoi le nombre de cas des utilisateurs qui sont victimes pour de l'hameçonnage continue à augmenter.**

Réponse

Mesure	Avantage(s)	Inconvénient(s)
Suppression des courriels suspects	Il n'y a pas de risque d'accéder aux faux sites web.	L'utilisateur ne sait pas toujours comment distinguer les courriels suspects.
Utilisation des filtres anti-spam	Après configuration les filtres fonctionnent de manière indépendante, l'utilisateur n'a plus a s'en soucié.	Les filtres anti-spam ne sont pas 100% fiables, il peut y avoir des faux positifs et faux négatifs. Si le filtre n'est pas là par défaut, l'utilisateur peut ne pas savoir comment configurer/ne pas connaître son existence.
Mise à jour régulière du mot de passe/Différents mot de passes par compte	Si on a été victime d'un hameconnage (conscient ou pas), l'attaquant n'a pas accès à d'autres de nos comptes et il	L'utilisateur doit penser à faire la mise à jour régulièrement et il doit garder en mémoire tous les différents

	pourra bientôt ne plus avoir accès au compte qui a été victime.	mot de passes associés aux comptes.
Accès à des informations sensibles en dehors d'un réseau public	En plus de l'hameconnage, on pourrait être victime d'une attaque MIIM sur un réseau public, donc ici on évite des failles multiques.	L'utilisateur doit attendre d'être sur un réseau privé pour l'accès.
Surveillance du contenu des liens	Sûr d'éviter l'hameconnage si on sait reconnaître les signes d'un lien malveillant.	Méthode pas 100% fiables. Il faut toujours être vigilant (ce qui n'est pas le cas si on pense déjà que le courriel vient d'une source sûre).
Configuration du navigateur pour éviter l'ouverture de sites trompeurs	Pareil que les filtres, après configuration cela fonctionne sans notre intervention. Nous n'avons pas à y penser et si on est sûr de la sûreté du site web on peut toujours y accéder en passant cette configuration de manière unique.	Il faut s'assurer de mettre à jour régulièrement le navigateur car la base de sites malveillants change vite. Aussi, faux positifs et faux négatifs existent, pas 100% fiable.

Le cas de victimes de hameconnage informatique augmente malgré les différentes mesures préventives existantes, car de plus en plus de personnes ont accès à internet, cela se démocratise chez les jeunes comme les plus âgés.
Toutefois la plupart de ces personnes ne sont pas éduqués au phishing. Même lorsque ces personnes en ont conscientes, on pense toujours que « cela n'arrive qu'aux autres » et on n'applique pas les mesures préventives conseillées car ce sont souvent des mesures qui demandent de la vigilance accrue ou du temps en plus.
De plus, les techniques des attaquants sont de plus en plus poussées. Par exemple, ils utilisent un profil de confiance lors du contact avec la victime. C'est-à-dire que sur Facebook par exemple, ils vont contacter les victimes en utilisant la fonction de messagerie avec un compte utilisateur qui est ami avec la victime. Cela apporte un sentiment de confiance et la victime est donc plus enclin à tomber dans le piège.