BUT 2

Thème 1 Droit des Données et Protection de la Vie Privée

TD1

DEPARTEMENT INFORMATIQUE

SUPPORTS TD

BUT 2

TD1 DECOUVRIR LE DROIT DES DONNEES ET LE RGPD… : LE CAS VOSREVES

La société VosRêves est spécialisée dans les voyages de luxe clef en main à destination des États-Unis et de la Polynésie Française. Elle se compose d'une maison mère située à Paris et de trois succursales situées à Bordeaux, Lyon et Marseille. L'entreprise, dirigée par M. Latour, existe depuis 1999 et s'est développée au fil des années. L'organigramme de la société vous est présenté en annexe 1.

Le système d'information de l'agence s'articule autour d'un Intranet[1] qui permet d'automatiser les activités de gestion des réservations et de gestion des voyages.

L'entreprise rencontre depuis deux ans un franc succès, grâce notamment à l'arrivée de nouvelles lignes aériennes directes entre la France et certains états américains, ainsi que vers la Polynésie.

De ce fait, l'embauche de plusieurs nouveaux salariés est prévue dans les différentes agences.

La protection du système d'information de l'entreprise

Face à cette augmentation du nombre de salariés, la sécurité des données personnelles numériques manipulées par l'entreprise devient cruciale. En effet, de nombreuses données nominatives sont stockées sur le serveur de données : des informations relatives aux clients et des informations bancaires des employés (RIB - Relevé d'identité bancaire – permettant de virer les salaires). L'entreprise dispose d'un réseau informatique sur lequel chaque employé se connecte avec un identifiant et un mot de passe qui lui ont été remis lors de l'embauche, et qui lui permettent d'accéder à toutes les données concernant les voyages proposés, ainsi qu'aux informations relatives aux clients.

Le mois dernier, le groupe a subi une attaque virale (sous la forme d'un envoi massif de courriers électroniques non désirés) qui n'a heureusement pas causé de dégâts importants, mais qui a prouvé la faiblesse de la sécurité informatique de l'intranet de l'entreprise.

Le responsable constate qu'il devient indispensable de sensibiliser les employés aux risques en matière de sécurité informatique : spam, hameçonnage, usurpation d'identité, virus, vol (tablettes, smartphones des commerciaux) ainsi qu'aux risques de sécurité interne (par négligence ou malveillance).

MISSION 1

À partir des vidéos citées ci-après et du site de la CNIL :

1/Décrire de manière structurée (tableau, carte heuristique, diagramme d'Ishikawa…) les différents types d'attaques existantes du système d'Information et dire en quoi elles peuvent concerner la société VosRêves.

Vidéos : https://www.cybermalveillance.gouv.fr/experience/

Vidéos : http://www.cigref.fr/cest-parti-pour-la-hack-academy-campagne-cybersecurite-du-cigref

CNIL : https://www.cnil.fr

2/ Citer les précautions à prendre pour limiter ces risques et rechercher des méthodes de protection adéquates.

3/ Réaliser des recherches afin d'expliquer comment l'entreprise pourrait former les employés à ces méthodes de protection.

[1] Intranet : réseau informatique interne à l'entreprise qui utilise les technologies d'Internet.

Les obligations de l'entreprise au regard de la conservation des données

Les données de l'entreprise sont à ce jour stockées sur le serveur centralisé de l'entreprise, dans les locaux du siège. Elles sont ensuite sauvegardées sur un serveur privé virtuel.

M. Latour avait à la création de l'entreprise déclaré à la CNIL tous les fichiers informatisés contenant des données à caractère personnel, comme celles de ces clients, employés et fournisseurs. Depuis l'administrateur du SI a pris le relai et s'est chargé des mises à jour nécessaires de ces déclarations.

Cependant, cette obligation légale a évolué. En effet, M. Latour a appris par son administrateur SI que depuis le 25 mai 2018 les entreprises doivent respecter le RGPD.

MISSION 2

À partir de recherches effectuées sur des sites de confiance et de l'annexe 2 :

4/ Expliquer en quoi consiste ce nouveau règlement et comment les entreprises doivent s'y conformer.

5/ Expliquer quels nouveaux types de risque menacent les entreprises et leurs conséquences pour celles-ci (cf. annexe 2).

Les nouveaux types d'attaques informatiques

Face à tous ces risques potentiels, M. Latour a organisé une formation de deux journées pour l'ensemble de ses salariés. Les nouveaux types d'attaques et le coût que cela peut représenter pour une entreprise ont été abordés lors de cette formation.

Il propose de s'inspirer des contenus exposés dans les articles suivants :

https://www.wimi-teamwork.com/fr/blog/chiffres-statistiques-marquants-cybersecurite/

https://www.latribune.fr/technos-medias/informatique/formjacking-malwares-modulables-les-menaces-cyber-des-entreprises-en-201-808538.html

MISSION 3

À partir des articles ci-dessus, présenter une synthèse des points abordés et concevoir un support de formation aux futurs employés.

Effectuer les recherches complémentaires nécessaires afin d'alimenter la synthèse avec des données récentes et pertinentes.

Évolutions concernant la sécurité des transactions

M. Latour a été très sensible aux difficultés financières rencontrées récemment par des tour-opérateurs pourtant réputés. Il se préoccupe notamment des différentes transactions financières opérées par son entreprise avec des acteurs qui ne sont pas systématiquement connus ou certifiés. En effet, suite aux catastrophes naturelles de plus en plus nombreuses, la société a dû annuler certains voyages et procéder au remboursement d'un grand nombre de ses clients au cours des dernières années. La procédure de remboursement utilisée à ce jour ne donne pas entièrement satisfaction à M. Latour qui souhaite trouver un système plus fiable.

M. Latour envisage notamment de mettre en place un système de sécurisation des transactions financières de l'entreprise avec ses différents partenaires (clients, fournisseurs, banques, assurances).

Il souhaiterait également pouvoir authentifier et protéger certains documents de l'entreprise comme les statuts juridiques, les contrats d'embauche, ceux signés avec les clients, etc.

Il a entendu parler de la technologie *blockchain* et vous demande si cette technologie pourrait répondre à ses besoins ?

Les articles suivants, l'interpellent plus particulièrement :

https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

https://www.journaldunet.com/solutions/expert/69574/blockchain---4-atouts-pour-votre-entreprise.shtml

https://www.lepoint.fr/technologie/mais-au-fait-c-est-quoi-la-blockchain-exactement-11-05-2019-2311973_58.php

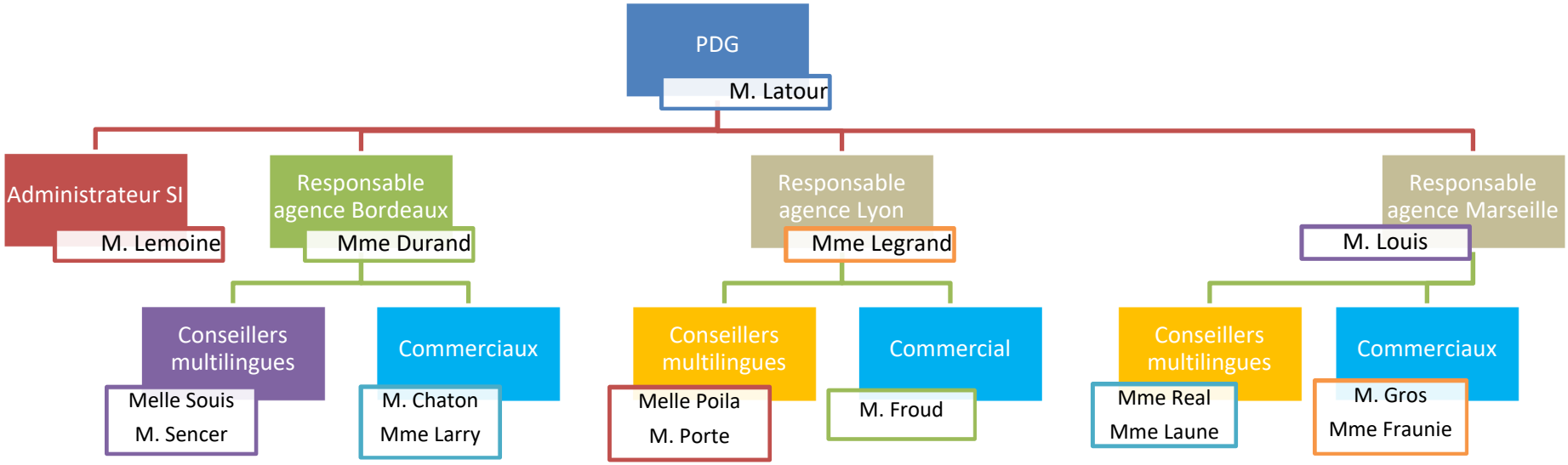
MISSION 4

À partir des articles ci-dessus, expliquez ce que la chaîne de blocs pourrait apporter à l'entreprise de M. Latour et si elle répond vraiment aux besoins exprimés.

Préciser si cette technologie remplacera réellement les tiers de confiance.

Annexes

Annexe 1 : Organigramme de la société



L'entreprise emploie à ce jour 15 salariés dont 6 conseillers multilingues chargés d'enregistrer les réservations auprès des clients et 5 commerciaux qui prospectent et organisent les voyages proposés à la vente. Les responsables d'agence gèrent la facturation et les paiements des voyages, ainsi que les relances clients. M. Latour s'occupe de la gestion du personnel et des fournisseurs ainsi que de la comptabilité de la société.

Annexe 2 : Les risques liés au RGPD

Le ransomhack surfe sur la vague du RGPD

http://www.itforbusiness.fr/thematiques/securite/item/10475-le-ransomhack-surfe-sur-la-vague-rgpd

Jacques Cheminat lundi, 25 juin 2018

La mise en œuvre du règlement européen sur la protection des données a titillé l'imagination des cybercriminels. Avec le *ransomhack*, ils ne bloquent plus les données, mais veulent les publier pour placer les entreprises victimes sous le coup des sanctions du RGPD.

Et les cybercriminels acquirent la fibre juridique en menaçant les entreprises d'écoper d'une sanction en cas de vol de données selon le RGPD. Cette réglementation est en vigueur depuis le 25 mai 2018 et prévoit en cas de vol de données des sanctions pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires de l'année précédente de l'incident.

La société de sécurité Tad Group a détecté une forme de *ransomware* d'une nature un peu différente des autres. Surnommé *ransomhack* par l'éditeur bulgare, il diffère du *ransomware* traditionnel au fait que les données ne sont pas bloquées, mais elles sont rendues publiques à moins qu'une rançon ne soit payée. En les rendant publiques, les cybercriminels placent les entreprises victimes sous le joug des sanctions du RGPD. Ce dernier impose aux sociétés d'assurer un haut niveau de protection sur les données.

1000 à 2000 dollars de rançon pour éviter une sanction RGPD

Les cyberpirates tentent donc de pousser les organisations à la faute et parient sur le fait que ces dernières préfèreront payer une rançon plutôt que de subir une enquête se traduisant par une sanction. L'équation économique est facile, payer une rançon comprise entre 1000 et 2000 dollars en cryptomonnaies ou risquer jusqu'à 20 millions de dollars ou 4% du chiffre d'affaires d'amende.

En même temps, payer la rançon comporte également un risque, car dans le RGPD, les entreprises victimes d'une violation de données ont 72 heures pour informer de l'incident. En cas d'oubli, elles peuvent être sanctionnées. Sans parler de la mauvaise publicité et de l'impact sur les clients.

Les cyberpirates surfent sur la vague du RGPD, car le terreau est favorable. Beaucoup d'entreprises sont en retard dans la mise en œuvre de la réglementation européenne et sont donc vulnérables. Certes les autorités de régulation sont bienveillantes à condition que les entreprises aient commencé à travailler sur la mise œuvre du RGPD.

Le *ransomware* ne faiblit pas

En France, le phénomène du *ransomware* progresse même si les plaintes se révèlent relativement faibles comme le montre le rapport sur l'état des cybermenaces du ministère de l'Intérieur. Sur l'année 2017, 420 procédures ont été déposées auprès des différents services de police et de gendarmerie. Un chiffre bas par rapport à la vague de WannaCry[2] qui a impacté beaucoup d'entreprises et non des moindres en France, Renault, Saint Gobain, etc.

On pensait que le RGPD allait augmenter le niveau de sécurité des entreprises. Par contre, on était loin d'imaginer qu'il pourrait servir de moyen de chantage pour obtenir une rançon...

[2] logiciel malveillant de type *ransomware* auto-répliquant.

Le RGPD, une bénédiction pour les cybercriminels et les arnaqueurs

https://www.latribune.fr/technos-medias/informatique/le-rgpd-une-benediction-pour-les-cybercriminels-et-les-arnaqueurs-783197.html

Sylvain Rolland | 27/06/2018

…

Autre fléau lié au RGPD : les escrocs qui jouent sur la peur des sanctions pour facturer une fausse mise en conformité. La Cnil a publié le 7 juin une mise en garde contre la recrudescence de cette pratique et a appelé entreprises et organisations à *"la plus grande vigilance"*.

Ainsi, certains escrocs envoient un faux formulaire intitulé "Déclaration normale RGPD", qui reproduit frauduleusement le logo de la Cnil. La victime doit remplir le fichier, le renvoyer, et payer pour la démarche.

Un autre cas de fraude est le fameux courrier, courriel ou fax de "dernier rappel", qui présente également un logo usurpé de la Cnil. Le message *"invite à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen"*, explique la Cnil. Qui en profite pour rappeler :

Pour aider les entreprises dans leur mise en conformité au RGPD, la CNIL a publié des guides et tutoriels comme "RGPD : ce qui change pour les pros", ou encore le "Guide de sensibilisation pour les petites et moyennes entreprises" élaboré en partenariat avec Bpifrance.