éduSCOL
Informer et accompagner les professionnels de l'éducation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

VOIE TECHNOLOGIQUE

Série STMG : Sciences et technologies du management et de la gestion

2DE | 1RE | TLE

Management, sciences de gestion et numérique

ENSEIGNEMENT
SPÉCIALITÉ

SÉCURITÉ ET CYBERCRIMINALITÉ

ENSEIGNEMENT COMMUN ET ENSEIGNEMENT SPÉCIFIQUE DE SYSTÈMES D'INFORMATION DE GESTION

Après une présentation de la ressource et la précision des repères dans les programmes de terminale, l'énoncé et le contexte sont présentés suivis de **4 parties**.

Deux documents (organigramme de la société et risques liés au RGPD) et plusieurs sitographies complètent l'énoncé et le contexte.

Enfin, un guide d'accompagnement pédagogique est proposé dans cette ressource.

Mots-clés

Sécurité informatique, cybercriminalité, cybersécurité, RGPD, CNIL, BlockChain, sécurité

Description du thème

Présentation de la ressource

Cette ressource permet aux élèves, placés dans le contexte d'une organisation, de découvrir les divers aspects de la sécurité et les moyens de protection face aux menaces informatiques.

Idéalement les élèves doivent travailler sur un poste de travail, seuls ou en binômes, pour les trois premières parties.

Durées indicatives :

- Partie 1 : 120 min
- Partie 2 : 30 min
- Partie 3 : 60 min
- Partie 4 : 30 min

La ressource peut être utilisée de façon à découvrir les notions qui y sont abordées ou bien comme une première illustration dans la séquence pédagogique de l'enseignant.

La ressource applique les préconisations du programme à savoir l'articulation entre l'observation, l'analyse, la conceptualisation et l'interprétation au travers d'un cas d'organisation dont les besoins ont été simplifiés.

La mobilisation des outils et ressources d'environnements numériques sont indispensables dans ce thème où, particulièrement, les technologies sont au cœur des transformations.

Aspects didactiques :
Si la plupart des questions peuvent être traitées individuellement par les élèves, certaines questions peuvent être traitées en binôme ou en groupe.

Cette ressource concerne le programme de l'enseignement de spécialité Management, Sciences de gestion et numérique, plus particulièrement celui de l'enseignement spécifique systèmes d'information de gestion. Sa mise en œuvre doit se faire en établissant des liens avec le tronc commun. Si deux enseignants se partagent le tronc commun et l'enseignement spécifique, il serait intéressant de travailler de façon collaborative les points du programme concernés.

Par exemple, une partie de cette ressource peut être travaillée dans le cadre de l'enseignement spécifique et exploitée également dans le cadre du tronc commun. Les élèves concernés peuvent exposer une synthèse de leurs travaux qui pourraient se poursuivre sous le regard des thèmes du tronc commun qui sont liés.

Repères dans les programmes de terminale

Programme de Management, Sciences de gestion et numérique : Enseignement commun

Thème 2 : Les organisations et les acteurs		
2.3 Communique-t-on de la même manière avec tous les acteurs ?	Identité de l'organisation : marque employeur, e-réputation, identité numérique.	Les possibilités offertes par les technologies numériques ont profondément modifié la manière dont les organisations appréhendent la communication. En combinant la communication sur différents médias numériques, l'organisation cherche à marquer sa présence et son identité tout en veillant à sa réputation.

Thème 3 : Les organisations et la société		
3.3. Les transformations numériques, de nouvelles responsabilités pour les organisations ?	Utilisation et protection des données personnelles et stratégiques. Transparence des algorithmes. Chaîne de blocs (*blockchain*).	Les transformations numériques offrent aux organisations de nouvelles occasions et peuvent toucher l'ensemble des chaînes de valeurs. Elles transforment les relations entre les citoyens et les organisations. L'exploitation des données personnelles oblige les organisations à respecter le règlement général sur la protection des données (RGPD). Les données stratégiques de l'organisation constituent un patrimoine qu'il convient de protéger. L'exploitation des données oblige les administrations à la transparence des algorithmes lorsqu'elles prennent des décisions concernant les individus. Le développement des chaînes de blocs (*blockchains*) modifie la sécurisation des échanges et la médiation des contrats. Cette question prolonge des éléments étudiés en classe de première dans l'enseignement de sciences de gestion et numérique et dans l'enseignement moral et civique, ainsi qu'en classe de seconde dans l'enseignement de sciences numériques et technologie.

Programme de Management, Sciences de gestion et numérique : Enseignement spécifique de systèmes d'information de gestion

Thème 1 : Organisation et numérisation		
1.2 Les évolutions numériques sont-elles exemptes de risques ?	Risques informatiques/ risques pour les individus. Sécurité du système d'information : finalités, démarche de sécurisation, outils et solutions. Protection des données et règlement général sur la protection des données (RGPD). Cybersécurité.	Le système d'information constitue une ressource stratégique pour les organisations. À ce titre, il faut le protéger en identifiant les risques associés susceptibles d'avoir des effets sur l'activité, en mesurer les conséquences et mettre en place une véritable démarche de sécurisation des processus et des équipements informatiques tout en respectant les obligations règlementaires. La sécurité des systèmes d'information s'entend à la cybersécurité pour prendre en compte les évènements issus du cyberespace qui sont susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données. Cela consiste, pour l'organisation, à prévenir les actes de malveillance délibérés ou la négligence avec intention de nuire ; cela exige des techniques nouvelles comme la mise en place d'une cyberdéfense pour lutter contre la cybercriminalité. Les données font l'objet d'une protection élevée, conformément aux obligations en la matière et aux avantages stratégiques et économiques qu'elles peuvent représenter.

Énoncé et contexte

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 dans le *document 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.

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

Partie 1 - 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. 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).

Travail à faire :
À partir de la sitographie indiquée ci-après :

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.
2. Citer les précautions à prendre pour limiter ces risques et rechercher des méthodes de protection adéquates.
3. Proposer des pistes permettant à l'entreprise de former les employés à la protection des données.

sitographie :

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

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

https://www.cnil.fr

Partie 2 - 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 ses 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.

Travail à faire :
À partir de recherches effectuées sur des sites de confiance et du document 2 :

1. Expliquer en quoi consiste ce nouveau règlement et comment les entreprises peuvent s'y conformer.
2. Expliquer quels nouveaux types de risques cela entraîne pour l'entreprise et leurs conséquences pour celle-ci (*document 2*).

Partie 3 - Les nouveaux types d'attaques informatiques

Face à tous ces risques potentiels, M. Latour pense organiser une formation de deux journées pour l'ensemble de ses salariés. Un bilan sur la cybercriminalité, un recensement des nouveaux types d'attaques et le coût que cela peut représenter pour une entreprise seront 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

Travail à faire :
À partir des articles ci-dessus :

1. 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.*

Partie 4 – 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

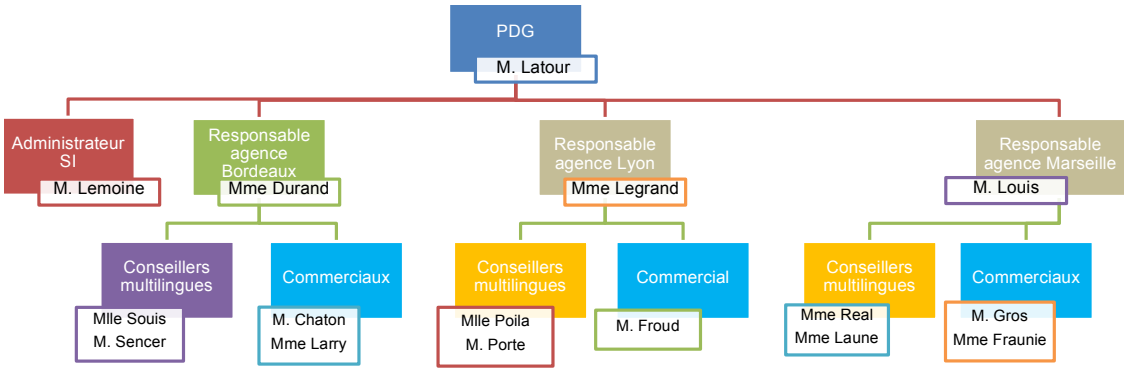
https://www.journaldunet.com/solutions/dsi/1418143-blockchain-4-atouts-pour-votre-entreprise/

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

> Travail à faire :
> À partir des articles ci-dessus :
>
> 1. Expliquer ce que la chaîne de blocs pourrait apporter à l'entreprise de M. Latour et si elle répond vraiment aux besoins exprimés.
> 2. Préciser si cette technologie remplacera réellement les tiers de confiance.

Ressources

Document 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.

Document 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...

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.

2. Logiciel malveillant de type *ransomware* auto-répliquant.

Guide d'accompagnement pédagogique

Partie 1 - La protection du système d'information de l'entreprise

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.

Les élèves pourraient faire en binôme la recherche d'un type d'attaque et proposer des solutions pour y faire face (questions 1 et 2). Puis chaque binôme pourrait exposer son travail au groupe classe et ainsi permettre un échange sur chaque type d'attaque évoqué.

On peut également envisager un travail par groupe de 3 ou 4 élèves chargés de traiter les 3 premières questions et de présenter de manière structurée leurs observations en classe.

Type d'attaque/ Risque	Fonctionnement	Objectif	Société VosRêves
Spam (attaque citée dans le sujet)	Réception de courrier électronique à des destinataires ne l'ayant pas sollicité.	Le but premier du spam est de faire de la publicité à moindre prix.	Un collaborateur peut recevoir des spams qui peuvent saturer et polluer sa boîte mail. Il peut ne pas recevoir ou supprimer ou encore ne pas lire un message important provenant d'un client. Le spam peut contenir un virus qui sera déployé sur le réseau à l'ouverture du mail.
Virus par messagerie	Réception d'un message avec pièce jointe activant un virus.	Détruire des données, bloquer l'ordinateur.	Un collaborateur peut recevoir ce type de mail et activer le virus en ouvrant la pièce jointe. Il met alors en péril les données de l'entreprise.
Rançongiciel	Réception d'un message avec pièce jointe activant un virus qui va bloquer votre ordinateur.	Vous faire payer une rançon avant de vous permettre de débloquer vos données.	Un collaborateur peut recevoir ce type de mail et activer le virus en ouvrant la pièce jointe. Les données de l'entreprise deviennent inaccessibles.
Piratage de téléphone mobile	Votre téléphone en veille est piraté.	Récupérer vos données, porter atteinte à votre réputation.	Un téléphone professionnel peut être piraté. Les données de l'entreprise sont en danger.
Récupération de mots de passe	Utiliser ses identifiants professionnels en se connectant sur un site frauduleux.	Récupérer les données des visiteurs du site.	Un collaborateur peut faire un achat en ligne depuis son poste de travail avec ses identifiants entreprise et mettre en péril les données de l'entreprise.

Rappel du lien cité précédemment : https://www.cigref.fr/cest-parti-pour-la-hack-academy-campagne-cybersecurite-du-cigref

Type d'attaque/ Risque	Fonctionnement	Objectif	Société VosRêves
Deviner un mot de passe (JENNY)	Tenter toutes les combinaisons habituelles (date naissance, date de mariage, ville, prénom d'un enfant ou animal…).	Récupérer le mot de passe de la messagerie d'un internaute afin par exemple de détourner ses virements bancaires.	Utiliser un mot de passe complexe (mélange de chiffres, lettres (minuscules/ majuscules), caractères spéciaux), mais dont vous pouvez vous souvenir et le changer régulièrement.
Phishing Hameçonnage (WILLY)	Envoyer un mail en se faisant passer pour un organisme connu (banque, assurance, …), en demandant au destinataire de fournir ses coordonnées.	Récupérer les coordonnées pour s'introduire dans le compte de l'abonné et pouvoir réaliser des virements bancaires en son nom ou celui de son entreprise.	Un collaborateur peut recevoir ce type de mail et divulguer des données confidentielles de l'entreprise.
Cheval de troie (MARTIN)	Insérer un code malveillant dans une application téléchargeable sur Internet. Une fois installé sur le pc du destinataire, le code récupère les mots de passe, les coordonnées bancaires… Autre méthode : laisser « trainer » des clés USB qui sont ensuite récupérées par les victimes de l'arnaque. La clé USB connectée au pc permet d'insérer le code malveillant.	Récupérer les données personnelles à l'insu de l'utilisateur. (*Sniffing*)	Un collaborateur peut télécharger un logiciel à usage personnel sur son poste de travail et faire entrer le cheval de Troie. Il peut aussi insérer une clef USB infectée sur un poste de travail de l'entreprise.
Interception d'échanges de données (DIMITRI)	Lors de l'achat sur un site non sécurisé, un pirate peut intercepter la communication et récupérer les coordonnées bancaires pour faire des virements frauduleux.	Récupérer des coordonnées bancaires pour voler de l'argent.	Un collaborateur peut faire un achat en ligne depuis son poste de travail avec les coordonnées bancaires de l'entreprise et mettre en péril la situation financière de l'entreprise.

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

À partir du lien cité en Q1 : https://www.cybermalveillance.gouv.fr/cybermenaces

Type d'attaque/ Risque	Précautions	Méthodes de protection adéquates
Spam	Ne pas ouvrir le mail car un virus peut être associé au spam. Ne pas acheter les produits proposés par le spam. Ne pas communiquer votre adresse email sur les forums ou les sites web car des robots parcourent automatiquement les sites web et collectent des adresses email pour les spammer.	Installer un anti-virus et un pare-feu et les mettre à jour régulièrement. Sensibiliser le personnel aux bonnes pratiques.
Virus par messagerie	Ne jamais ouvrir un mail douteux ou dont on ne connait pas la provenance.	Installer un anti-virus et un pare-feu et les mettre à jour régulièrement. Formation du personnel : sensibilisation à la cybercriminalité. https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
Rançongiciel	Ne jamais ouvrir un mail douteux ou dont on ne connait pas la provenance. N°1 des attaques en France en 2018 : https://www.silicon.fr/cybersecurite-le-ransonware-n1-des-attaques-en-france-222855.html	Installer un anti-virus et un pare-feu et les mettre à jour régulièrement. Sauvegarder régulièrement les données. https://www.cnil.fr/fr/securite-sauvegarder-et-prevoir-la-continuite-dactivite Formation du personnel : sensibilisation à la cybercriminalité (ne jamais payer la rançon, mais déposer plainte).
Téléphone mobile	Assurer la sécurité de votre téléphone : par blocage rapide, mot de passe complexe, et ne jamais le laisser sans surveillance.	Formation du personnel. Paramétrage des téléphones de l'entreprise : blocage rapide et à distance si nécessaire. https://www.cnil.fr/fr/securite-securiser-linformatique-mobile
Mots de passe	Utiliser un mot de passe spécifique pour votre messagerie professionnelle. Utiliser des identifiants et des mots de passe différents et complexes pour votre navigation web. Les renouveler régulièrement. (Cf vidéo du cigref : Jenny)	Obliger le personnel à changer de mot de passe très régulièrement et à utiliser des mots de passe suffisamment complexes (long et comprenant des caractères spéciaux). https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail

À partir du lien cité en Q1 : http://www.cigref.fr/cest-parti-pour-la-hack-academy-campagne-cybersecurite-du-cigref

Type d'attaque/ Risque	Précautions	Méthodes de protection adéquates
Phishing Hameçonnage (WILLY)	Ne pas suivre les liens et ne pas ouvrir les pièces jointes des mails suspects (expéditeur inconnu, pas d'objet, objet en anglais…). Ne jamais fournir de coordonnées bancaires ou mot de passe par mail.	Installer un anti-virus et un pare-feu et les mettre à jour régulièrement. Formation du personnel : sensibilisation à la cybercriminalité. https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant
Cheval de troie (MARTIN)	N'utiliser pas de logiciels ni de clé USB de sources incertaines.	Blocage de l'usage des clés USB (ports USB des ordinateurs bloqués) et des téléchargements. Mise en place d'anti-virus tenu à jour. Sauvegarde régulière des données. https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail
Interception d'échanges de données (DIMITRI)	Lors d'achat, toujours vérifier la présence du https : s signifiant sécurisé (chiffrement des données).	Usage du protocole TLS (*Transport Layer Security*) : procédé de sécurisation des transactions effectuées via Internet, basé sur le chiffrement. https://www.cnil.fr/fr/securite-securiser-les-sites-web

3. Proposer des pistes permettant à l'entreprise de former les employés à la protection des données.

Les élèves pourraient proposer de mettre en place systématiquement la sensibilisation à la sécurité des informations (*e-learning*, jeux-sérieux, ateliers...) à l'arrivée de nouveaux collaborateurs.

Ils peuvent également proposer des jeux sous forme de simulation d'attaques.

Faire signer à l'embauche la **charte informatique** de l'entreprise et mettre celle-ci en évidence dans les locaux, pour rappel, puis former les salariés sur les points suivants :

- le verrouillage du poste de travail (ou du téléphone) pour empêcher qu'un tiers n'y accède ;
- le danger de connecter des équipements personnels au réseau de l'entreprise ;
- le secret des mots de passe ;
- le danger des pièces jointes dans les courriels, ainsi que les conséquences des e-mails frauduleux et des achats en ligne.

On peut également :

- diffuser des **notes de service** au personnel (panneau d'affichage ou messagerie interne par exemple) pour rappel des bonnes pratiques en termes de sécurité informatique ;
- proposer des **cours en *e-learning*** aux salariés. Ils devront obligatoirement visualiser ces cours en ligne à leur arrivée dans l'entreprise, puis ponctuellement en fonction des nouveaux besoins repérés par la direction.
- proposer des **jeux sérieux** aux salariés. Exemple : http://www.cigref.fr/sensibiliser-a-la-cybersecurite-le-serious-game-cigref-dans-les-entreprises
- Organiser des **ateliers de sensibilisation**

http://bfmbusiness.bfmtv.com/01-business-forum/cinq-methodes-pour-sensibiliser-vos-salaries-a-la-securite-597505.html

Inviter un intervenant externe à l'entreprise pour présenter son expérience et ses mésaventures avec la sécurité informatique (obtenir si possible la visite gratuite d'un expert de la Direction centrale du renseignement intérieur (DCRI), ou de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Afin de valider l'efficacité de votre campagne de sensibilisation, vous pouvez « **piéger vos salariés** ». Pour cela, déposez dans les salles de repos, ascenseurs, couloirs ou parkings une clé USB. Pour que vos collaborateurs ne résistent pas à l'envie de s'en emparer, utilisez une clé USB de grande capacité, assez onéreuse.

Dessus, enregistrez un fichier au nom évocateur comme " salaires.doc ". Il s'agira en l'occurrence d'un fichier dans lequel vous aurez copié-collé le lien vers une page invisible de votre site Web.

Si l'utilisateur clique sur ce lien, parce que vous aurez inséré juste avant une phrase du style " Monsieur le directeur, veuillez trouver ci-dessous le lien vers la page qui référence tous les salaires de l'entreprise ", son navigateur ouvrira la page en question et son adresse IP s'inscrira dans les relevés d'activité de votre site Web. Relevés qu'il suffira ensuite de lire pour savoir quel poste de l'entreprise a commis l'imprudence d'utiliser la clé USB.

L'opération nécessite la complicité de l'informaticien en charge du site Internet, qui bâtira pour vous la page fantôme et vous fournira le relevé des connexions. Idéalement, il programmera cette page fantôme pour qu'elle affiche le nom de l'employé imprudent (d'après son adresse IP), suivi de " Vous avez été piégé ". Cette ruse, inoffensive, montre qu'un salarié aurait pu introduire involontairement de la même manière un virus sur le réseau.

Ce guet-apens est déclinable en **campagne de *phishing***, c'est-à-dire en envoyant aux salariés des courriels maquillés aux couleurs de leur banque les incitants à cliquer pour entrer des informations secrètes. Avec toujours pour but d'arriver sur la page révélant le piège sur votre site Internet. Bien sûr, l'e-mail ne sera pas expédié depuis une adresse de l'entreprise : créez une adresse anonyme sur Gmail par exemple.

A l'issue de ces tests, vous pourrez **révéler via votre messagerie interne l'existence de ces pièges** et indiquerez que des salariés ont été pris la main dans le sac. Vos collaborateurs seront ainsi incités à plus de prudence. Mais n'enlevez pas pour autant vos pièges. Prévenez vos employés qu'en cas de récidive, ils devront repasser par la case **" formation et test des connaissances "**.

Enfin, le " **jeu des croissants** " fonctionne aussi très bien pour inciter à la vigilance. Lorsqu'un collaborateur s'absente de son poste, ses collègues vérifient qu'il a pensé à verrouiller son écran. Si ce n'est pas le cas, on se sert de son PC pour envoyer à tout l'étage un message intitulé " Demain j'apporte les croissants ". En général, un salarié n'est piégé qu'une seule fois !

Partie 2 - Les obligations de l'entreprise au regard de la conservation des données

1. Expliquer en quoi consiste ce nouveau règlement et comment les entreprises peuvent s'y conformer.

https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-internaute.html

Le Règlement général sur la protection des données (RGPD ou GDPR, pour General data protection regulation en anglais) est le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces informations sur lesquelles les entreprises s'appuient pour proposer des services et des produits. Ce texte couvre l'ensemble des résidents de l'Union européenne.

L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles, en remplaçant une directive datant de 1995. Une réforme de la législation européenne apparaissait nécessaire au regard de sa relative vétusté, accentuée par l'explosion du numérique et l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques.

Depuis le 25 mai 2018, tout traitement en infraction avec le RGPD peut déboucher sur des sanctions.

https://www.cnil.fr/fr/rgpd-par-ou-commencer

Voici les 4 actions principales à mener pour assurer la mise en conformité aux règles de protection des données. Ces actions doivent perdurer dans le temps pour être efficaces.

- Constituer un registre de vos traitements de données afin de recenser tous vos fichiers et d'avoir une vision d'ensemble.
- Faire le tri dans vos données pour ne conserver que celles dont vous avez réellement besoin.
- Respecter les droits des personnes en respectant l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).
- Sécuriser vos données.

2. Expliquer quels nouveaux types de risques cela entraîne pour l'entreprise et leurs conséquences pour celle-ci (document 2).

https://www.oodrive.fr/blog/securite/ransomhack-comment-faire-du-rgpd-une-nouvelle-arme-contre-les-entreprises/

Les sanctions prévues par le RGPD sont une véritable incitation à être en conformité avec le texte. Les amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du CA annuel ont en tous cas donné des idées aux cyberpirates. Un ransomware d'un nouveau genre a fait son apparition. Les entreprises sont désormais confrontées au ransomhack.

Le ransomware est un programme malveillant dont le but est d'obtenir une rançon en empêchant l'utilisateur d'accéder à ses données, ces dernières étant chiffrées. Mais la société de cybersécurité bulgare Tad Group a révélé une nouvelle forme d'extorsion. Dans le cas du ransomhack, les données ne sont pas bloquées si l'entreprise ne paye pas la rançon. Elles sont rendues publiques. Une variante qui a vu le jour avec l'entrée en vigueur du règlement européen.

Si les pirates informatiques surfent sur la vague du RGPD, ce n'est pas par hasard. Le texte est entré en application le 25 mai dernier. Pourtant, aujourd'hui encore, de nombreuses entreprises ne sont toujours pas en conformité. De nombreux experts en cybersécurité estiment que les entreprises préfèreront payer les rançons et rester discrètes quant aux éventuels incidents dont elles sont victimes. Elles échappent ainsi aux amendes prévues par le texte européen.

La législation considère qu'il y a eu violation de données à caractère personnel en cas de perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite. La notification de l'incident doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

Le règlement européen prévoit que toute fuite de données doit être signalée dans les 72h après la découverte de l'incident. D'après la société Tad Group, les rançons demandées dans le cadre d'un ransomhack sont comprises entre 1 000 et 20 000 dollars. Compte tenu du niveau des sanctions, payer les cyberpirates semble être une solution moins onéreuse pour une entreprise.

Le ransomhack entraine donc un risque financier non négligeable pour les entreprises.

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

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».

Autre conséquence : Les arnaques à la conformité se multiplient et augmentent le risque financier pour les entreprises.

Partie 3 - Les nouveaux types d'attaques informatiques

1. 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.*

Résumé attendu en trois points :

- Bilan sur la cybercriminalité aujourd'hui dans les entreprises

https://www.commentcamarche.net/news/5872314-cybercriminalite-en-france-les-chiffres-officiels

http://www.leparisien.fr/economie/cybercriminalite-les-entreprises-francaises-de-plus-en-plus-attaquees-18-04-2019-8055717.php

Nouvelles attaques à recenser et expliquer : l'arnaque au président, le shadow IT, la vulnérabilité résiduelle, le formjacking, le cryptojacking, malwares « modulables », les objets connectés et systèmes mobiles plus vulnérables.

https://www.journaldunet.com/solutions/expert/70751/tout-savoir-sur-l-arnaque-au-president.shtml

https://fr.wikipedia.org/wiki/Shadow_IT

https://www.silicon.fr/cybersecurite-le-ransonware-n1-des-attaques-en-france-222855.html

- Vulnérabilité résiduelle : Seuil minimal de vulnérabilité atteint par un système après que l'on a effectué l'évaluation de sa vulnérabilité, l'analyse des causes de menaces informatiques et la mise en place des contre-mesures de sécurité informatique appropriées

https://www.developpez.com/actu/249094/Symantec-le-formjacking-constitue-la-nouvelle-forme-d-attaque-utilisee-par-les-pirates-pour-s-enrichir-encore-plus-vite-qu-avec-les-ransomwares/

https://www.journaldunet.com/solutions/expert/68748/le-cryptojacking--virus-createur-de-cryptomonnaie.shtml

https://gblogs.cisco.com/fr/securite/nouveau-rapport-cisco-cybersecurite-2019-decryptage-dune-annee-agitee-et-petits-conseils-dami-pour-lavenir/

https://www.latribune.fr/technos-medias/internet/cybersecurite-les-objets-connectes-et-les-systemes-industriels-de-plus-en-plus-attaques-805175.html

- Coût de la cybercriminalité en France et dans le monde :

https://www.lesechos.fr/tech-medias/hightech/le-cout-des-cyberattaques-explose-partout-dans-le-monde-1005615

Partie 4 – Évolutions concernant la sécurité des transactions

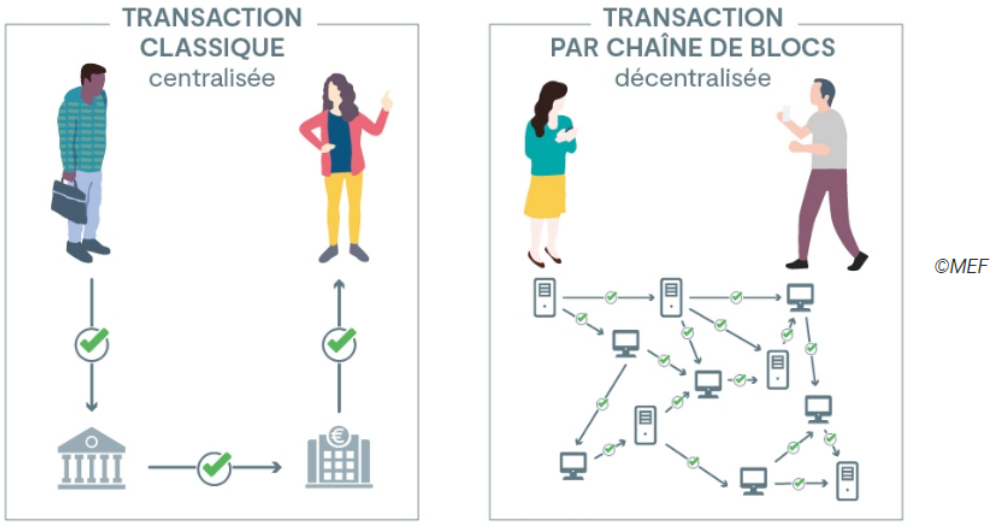
1. Expliquer ce que la chaîne de blocs pourrait apporter à l'entreprise de M. Latour et si elle répond vraiment aux besoins exprimés.

Définition

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

Développée à partir de 2008, la blockchain est une technologie de stockage et de transmission d'informations, prenant la forme d'une base de données, qui a la particularité d'être partagée simultanément avec tous ses utilisateurs et qui ne dépend d'aucun organe central.

Elle a pour avantage d'être rapide et sécurisée et son champ d'application est bien plus large que celui des cryptomonnaies/cryptoactifs (assurance, logistique, énergie, industrie, santé, etc.).



©MEF

La **sécurité du système** est assurée par le fait que la validation est effectuée par un ensemble d'utilisateurs différents, qui ne se connaissent pas. Cela permet de se prémunir du risque de malveillance ou de détournement, puisque les nœuds surveillent le système et se contrôlent mutuellement.

La sécurité des transactions

https://www.lesechos.fr/idees-debats/cercle/blockchain-optimiser-la-securite-des-donnees-et-redonner-le-controle-aux-utilisateurs-137517

La blockchain permet d'apporter un niveau de sécurité inégalé à des événements, des titres de propriété, des archives financières, médicales ou juridiques, des connexions IoT (Internet des objets), des activités de gestion, la vérification des processus, les transferts de données, la gestion des identités, le traitement des transactions, la traçabilité…

L'automatisation des remboursements
https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

La blockchain permet l'automatisation des procédures de remboursement et l'allégement de certaines formalités à la charge des sociétés comme de leurs clients sous réserve que les hypothèses et les conditions d'indemnisation et de préjudice soient clairement établies.

La protection des documents internes
https://www.journaldunet.com/solutions/expert/69574/blockchain---4-atouts-pour-votre-entreprise.shtml

La blockchain permet à chaque acteur de la chaîne de certifier que les documents ou les actions soient authentiques, assurant ainsi leur caractère officiel.

Dans le domaine de l'immobilier, la blockchain est utilisée pour authentifier les actes de propriété ou l'état des propriétés foncières des individus. Dans le domaine de l'éducation, le MIT s'équipe de la blockchain pour éditer numériquement les diplômes de ses étudiants, permettant de les valider officiellement auprès des organismes qui en auraient besoin.

L'archivage est indispensable dans toute activité pour conserver un historique des actes, des actifs, des produits ou encore des événements.

La blockchain constitue un registre de façon automatique, validé par des organismes officiels, et mis à disposition de tous, même des utilisateurs finaux.

Conclusion
Cette technologie semble en effet répondre aux besoins de M. Latour. Il devra s'adresser à son administrateur de SI ou un autre spécialiste afin de mettre en place sa chaine de blocs.

https://www.journaldunet.com/solutions/cloud-computing/1206814-comment-mettre-en-oeuvre-une-blockchain/

Mais d'autres solutions sont possibles :
https://www.hexatrust.com/solutions/securisation-des-transactions/

2. Préciser si cette technologie remplacera réellement les tiers de confiance.
https://fr.wikipedia.org/wiki/Tiers_de_confiance

Un tiers de confiance est une personne physique ou morale habilitée à effectuer des opérations de sécurité juridique d'authentification, de transmission et de stockage.

Le terme est employé notamment, mais pas exclusivement, pour désigner les professionnels habilités à mettre en œuvre des signatures électroniques.

Cette dénomination est employée dans plusieurs domaines différents : l'échange de biens, l'authentification et la transmission de documents dématérialisés, l'échange d'informations sur internet, les déclarations fiscales françaises :

1. Protection des transactions de biens contre des paiements : par exemple Paypal, Vérifdeal, PriceMinister ou Amazon.
2. Protection automatique par certificat informatique, dit aussi électronique, lors des échanges sur internet (sécurisation des pages web, des courriers, des fichiers exécutables).
3. Délégation de déclaration fiscale et représentation auprès des services de l'état.

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

Cette technologie remplacera-t-elle réellement les tiers de confiance ?

Oui et non. Dire que la blockchain va remplacer tous les tiers de confiance est exagéré. Cette technologie va plutôt permettre d'identifier quelle est la vraie valeur ajoutée de ces tiers de confiance. Par exemple, les banques ne se limitent pas à faire des transferts d'argent, elles fournissent également des services ajoutés qui ont une valeur pour les clients. Cependant, ces services reposent sur des autorités de confiance et une infrastructure gouvernée de façon centralisée.