

Les enjeux de la cybersécurité au sein des PME suisses ayant un faible degré de digitalisation

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Lucas LE BRETON

Conseiller au travail de Bachelor :

Roland SAKO

Genève, 22 juillet 2024

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science HES-SO en Informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son directeur de mémoire afin qu'il l'analyse à l'aide du logiciel de détection de plagiat COMPILATIO.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Archamps, le 22/07/2024

Lucas Le Breton

Remerciements

Pour réduire les fautes d'orthographe et améliorer la syntaxe grammaticale, de nombreux paragraphes de ce document ont été retravaillés à l'aide de l'intelligence artificielle, notamment celle d'OpenAI.

Je remercie le studio d'enregistrement Origine Sounds Records, Helvetcontrol SA et l'ancienne responsable du restaurant Chez Marie Chou pour leur participation active, notamment en testant mon application et en fournissant des retours à la fois oralement et aussi grâce au formulaire de feedback.

Résumé

Ce travail de Bachelor se concentre sur les défis de la cybersécurité auxquels font face les petites et moyennes entreprises (PME) suisses, particulièrement celles ayant un faible degré de digitalisation. L'objectif principal est de développer une solution innovante sous format de Proof of Concept afin de fournir des conseils personnalisés en cybersécurité adaptés aux spécificités de chaque PME.

La méthodologie utilisée comprend une analyse du degré de digitalisation des PME suisses, l'identification des principales menaces et vulnérabilités en cybersécurité, et l'examen des bonnes pratiques actuelles. Un questionnaire a été développé pour évaluer les pratiques de sécurité des PME, et les réponses ont été analysées à l'aide de l'intelligence artificielle générative d'OpenAI pour fournir des recommandations personnalisées.

Les tests effectués avec trois responsables de PME genevoises ont montré que les utilisateurs trouvaient les conseils pertinents et applicables, bien que certaines redondances et variations dans les conseils générés aient été notées. La solution proposée est jugée plus accessible financièrement par rapport aux solutions concurrentes, avec un coût d'utilisation très faible.

Cette étude met en évidence l'importance de la cybersécurité pour les PME et l'intérêt de solutions personnalisées. Les améliorations futures de la solution incluent l'optimisation des prompts, la mise en ligne de la solution, l'intégration de modèles locaux d'IA, et l'amélioration de la mise en page des documents générés. Le projet a permis de démontrer la valeur d'une approche personnalisée pour renforcer la sécurité numérique des PME suisses.

En poursuivant le développement de cette application, il est possible d'apporter une aide significative aux PME pour qu'elles renforcent leur cybersécurité de manière efficace et économique. La solution présente des perspectives prometteuses pour devenir un outil incontournable dans le domaine de la sécurité informatique pour les PME peu digitalisées.

Table des matières

Déclaration.....	II
Remerciements	III
Résumé	IV
Liste des tableaux	IX
Liste des figures.....	IX
1. Chapitre 1 : Introduction	1
2. Chapitre 2 : Panorama de la digitalisation au sein des PME suisses ...	2
2.1 Définition des PME en Suisse	2
2.2 Digitalisation des PME suisses	2
2.2.1 C'est quoi la digitalisation ?	2
2.2.2 État actuel	3
2.3 Facteurs influençant le degré de digitalisation.....	4
2.3.1 Interne.....	4
2.3.2 Externe	5
2.4 Évaluation de la digitalisation	6
2.4.1 Infrastructure et technologie	6
2.4.1.1 Matérielle	6
2.4.1.2 Immatérielle	6
2.4.1.2.1 Software	6
2.4.1.2.2 Formation des employés	6
2.4.1.2.3 Présence en ligne.....	6
2.4.2 Processus et workflow.....	7
2.4.3 Gouvernance numérique.....	7
2.4.3.1 Sécurité	7
2.4.3.2 Gestion des données.....	7
3. Chapitre 3 : Les défis de la cybersécurité pour les PME suisses	8
3.1 Importance de la cybersécurité pour les PME	8

3.2	Les principales menaces et vulnérabilités	8
3.2.1	Ingénierie sociale/OSINT	8
3.2.1.1	Qu'est-ce que c'est l'ingénierie sociale ?	8
3.2.1.2	Rôle de l'OSINT dans l'ingénierie sociale	9
3.2.2	Ransomware	10
3.2.3	DDOS	10
3.3	Impacts potentiels des cyberattaques sur les PME.....	11
3.3.1	Fuite de données	11
3.3.2	Espionnage	11
3.3.3	Financier	12
3.3.4	Image publique.....	12
3.3.5	Légal	12
3.4	Méthodes d'analyse des menaces	13
3.4.1	Méthode STRIDE	13
3.4.2	Méthode TRIKE.....	14
3.4.3	Méthode DREAD.....	14
4.	Chapitre 4 : Bonnes pratiques et mesures.....	15
4.1	État de l'art	15
4.2	Obstacles à la mise en place de mesures de sécurités.....	16
4.3	Lacunes et zones d'amélioration	16
4.4	Possible mitigations supplémentaires	16
4.4.1	Stratégies de sensibilisation axées sur l'ingénierie sociale	16
4.4.2	Cas réels déjà passé en Suisse	18
4.4.3	Proposition de mesures supplémentaires.....	18
4.5	Que faire en cas d'attaque ?.....	19
4.5.1	Bonne pratique.....	19
4.5.2	Ce qu'il ne faut pas faire.....	20
4.5.3	Réponse à incident	20

5. Chapitre 5 : Solution proposée : Conseils personnalisés	21
5.1 Informations générales.....	21
5.2 Utilisation de l'IA générative	22
5.3 Structure de la solution	23
5.3.1 Dossier « resultats »	23
5.3.2 Dossier « src »	23
5.3.3 Dossier « templates ».....	23
5.3.4 Dossier « static ».....	23
5.4 Questionnaire.....	23
5.4.1 Infrastructure et technologie	23
5.4.1.1 Matériel.....	23
5.4.1.2 Stockage des données.....	24
5.4.1.3 Partage des données	24
5.4.2 Logiciels.....	25
5.4.3 Formation des employés	25
5.4.4 Présence en ligne	26
5.4.5 Sécurité des systèmes	27
5.4.5.1 Outils.....	27
5.4.5.2 Réseaux wifi	27
5.4.6 Réactions en cas d'attaque	28
5.4.7 Cas concret.....	29
5.5 Résultat.....	29
5.5.1 Remarques personnelles	29
5.5.2 Analyse feedback utilisateur.....	30
5.5.2.1 Résultat formulaire	30
5.5.2.1.1 Quantité des conseils fournis	30
5.5.2.1.2 Pertinence des conseils fournis	31
5.5.2.1.3 Application des conseils fournis	32
5.5.2.1.4 Interprétation globale des résultats	32

6. Chapitre 6 : Conclusion	33
6.1 Digitalisation	33
6.2 Cybersécurité	33
6.3 Bonnes pratiques.....	34
6.4 Solution	34
6.4.1 Limite de la solution	35
6.4.2 Perspective de la solution	36
6.5 Avis personnel	37
Bibliographie	38
Annexe 1 : Exemple plan de capacités fonctionnelles	43
Annexe 2 : Exemple des conseils générés	44

Liste des tableaux

Tableau 1 - Librairies python	22
-------------------------------------	----

Liste des figures

Figure 1 - Considération de la digitalisation par les artisans suisses	3
Figure 2 - Externalisation des taches informatiques	15
Figure 3 - Réponse formulaire, question 1	30
Figure 4 - Réponse formulaire, question 2	31
Figure 5 - Réponse formulaire, question 3	32
Figure 6 - Coût mensuel en centimes	35

1. Chapitre 1 : Introduction

La transformation numérique est devenue un facteur déterminant pour la compétitivité et la survie des petites et moyennes entreprises (PME) dans le paysage économique actuel. En Suisse, où les PME constituent la colonne vertébrale de l'économie en jouant un rôle majeur pour le pays, leur degré de digitalisation revêt une importance particulière. Cependant, la digitalisation apporte son lot de défis, notamment en matière de cybersécurité. Les PME suisses, souvent limitées en ressources humaines et financières, se retrouvent confrontées à des menaces croissantes qui peuvent compromettre leur viabilité.

Dans un premier temps, nous examinerons la définition d'une PME et celle de la digitalisation. Ensuite, nous analyserons l'état actuel de la digitalisation, les facteurs qui l'influencent, ainsi que les méthodes pour l'évaluer.

Dans un second temps, nous nous concentrerons sur les défis en matière de cybersécurité auxquels les PME suisses peuvent faire face. Nous mettrons en avant :

- l'importance de la cybersécurité
- les principales menaces et vulnérabilités
- les impacts potentiels sur une PME
- les méthodes d'analyse des menaces.

Dans un troisième temps, nous nous pencherons sur les bonnes pratiques et les mesures qu'une PME peut adopter pour renforcer sa cybersécurité. Nous commencerons par un état de l'art, tout en identifiant les obstacles à la mise en place de mesures de sécurité rencontrés par les PME. Cela nous permettra de détecter les lacunes et les domaines à améliorer, afin de proposer des solutions complémentaires.

Enfin, nous présenterons une proposition de solution offrant des conseils personnalisés en fonction de la situation spécifique de chaque PME. Cette solution consiste en une application web qui propose un questionnaire pour évaluer globalement la situation d'une PME. Les réponses sont analysées par une intelligence artificielle générative pour fournir des recommandations personnalisées. Nous mettrons en avant dans ce document les informations générales liées à ce projet, la structure de celui-ci, détaillerons comment nous utilisons l'IA, comment est établi le questionnaire, et concluons par une analyse des résultats que cette solution peut offrir.

2. Chapitre 2 : Panorama de la digitalisation au sein des PME suisses

2.1 Définition des PME en Suisse

L'acronyme PME provient de « petite-moyenne entreprise ». Les critères européens pour définir une PME sont la taille de l'entreprise, qui doit être inférieur à 250 employés et un critère financier qui accepte soit un chiffre d'affaires annuel inférieur à 50 millions d'euros soit un total du bilan de 43 millions d'euros. (*Confédération Suisse 2024a*)

Cependant, en Suisse, selon le secrétariat d'État à l'économie qui est une office fédéral ayant pour principal objectif de maintenir une croissance économique pérenne (*Confédération Suisse 2024b*), les PME sont seulement définies par leur taille en terme d'employé. Il n'y pas de critère financier. Les petites et moyennes entreprises suisses sont donc toutes les entreprises ayant entre 1 et 249 employés.

En termes de répartition nationale, les petites et moyenne entreprises couvre plus de deux tiers des emplois. Sachant que 99% des entreprises suisse sont des PME. (*Confédération Suisse 2024c*)

2.2 Digitalisation des PME suisses

2.2.1 C'est quoi la digitalisation ?

Au cours de l'histoire, nous avons pu observer 4 grandes révolutions industrielles :

- La première au XVIIIème siècles, marquée par l'introduction de la machine à vapeur, qui a révolutionné la production en permettant l'utilisation de machines.
- La seconde révolution à la fin du XIXème lié à la production de masse par le biais de l'électricité et du pétrole.
- La troisième en 1969 avec l'automatisation de la production grâce à l'électronique et des technologies informatique.
- La quatrième est en cours et elle est orchestré par entre autres l'intelligence artificielle, l'internet des objets et le cloud.

Ces nouvelles technologies offrent aux entreprises la capacité de s'adapter et de répondre aux défis contemporains. (*Retail 2022*)

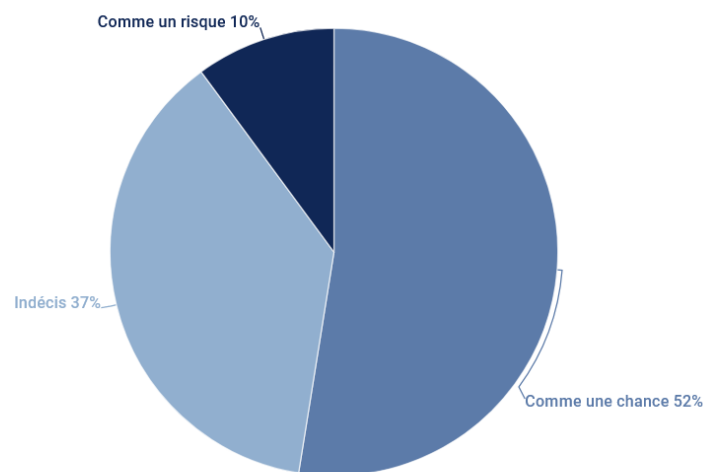
La digitalisation est donc le phénomène d'adapter les outils et les méthodes d'hier afin de répondre aux nouveaux défis émergents d'aujourd'hui.

2.2.2 État actuel

La digitalisation devient de plus en plus cruciale pour les PME, avec une prise de conscience notable entre 2017 et 2019, période durant laquelle on note une augmentation de 28% des entreprises reconnaissant l'importance des technologies numériques. Bien que ces statistiques remontent à quelques années, l'augmentation constatée montre un intérêt grandissant pour la numérisation. (*Le Monde Économique 2019*)

Près de 47 % des acteurs dans le secteur de l'artisanat montrent une méconnaissance des enjeux de la digitalisation. Entre ceux qui y voient un risque, représentant environ 10 %, et ceux encore indécis, à hauteur de 37 %, il est clair qu'il reste beaucoup à faire pour que toutes les PME perçoivent la digitalisation comme une opportunité pour leurs activités. (*Wagner, Kindle 2020*)

Figure 1 - Considération de la digitalisation par les artisans suisses



(Wagner, Kindle 2020)

2.3 Facteurs influençant le degré de digitalisation

Divers éléments peuvent avoir un impact sur la digitalisation des petites et moyennes entreprises suisses. On retrouve des défis internes à l'entreprise mais aussi des défis externes.

2.3.1 Interne

La digitalisation relève un aspect sous coté dans les entreprises. Elle est souvent vue comme un coût ou bien une charge au lieu d'être perçu comme un investissement. Le manque de ressource financière peut constituer un des principaux freins à la numérisation d'une entreprise. *(Le Monde Économique 2019)*

En plus de disposer des ressources nécessaires, une entreprise doit également veiller à ce que ses employés soient qualifiés pour utiliser les nouveaux outils qui amélioreront les processus existants. Il est primordial de former le personnel, que ce soit pour une initiation ou de façon continue. L'investissement pour la formation peut représenter une dépense considérable en termes de temps et d'argent, des ressources qui ne sont pas toujours disponibles, en particulier dans les petites et moyennes entreprises.

Le conservatisme peut aussi ralentir et influencer la numérisation d'une entreprise. Cette approche idéologique affecte la culture d'entreprise, qui doit s'adapter pour favoriser un management moins exécutif et assouplir les méthodes de travail actuelles. Cela est perceptible dans la réticence de certains employeurs à permettre le travail à distance, souvent due à un manque de confiance qui révèle une absence d'habitude en la matière. Cette philosophie de vie peut également nous contraindre à maintenir des structures hiérarchiques traditionnelles et verticales. Ces structures ne favorisent pas l'agilité nécessaire pour intégrer et mettre en œuvre les nouvelles méthodes de travail associées à la digitalisation. Adopter des structures holacratiques, où des spécialistes remplacent les responsables, pourrait répondre à ce besoin d'agilité *(CSEM 2023)*.

L'accès à et la possession de certaines infrastructures technologiques facilitent également la digitalisation rapide des entreprises. En effet, une entreprise équipée de la fibre optique, de smartphones et de laptops de dernière génération ou presque, est mieux positionnée pour se numériser. Ainsi, les régions et les entreprises les mieux équipées sont susceptibles de se digitaliser plus rapidement et plus efficacement.

2.3.2 Externe

Le fait qu'un concurrent d'une PME adopte une nouvelle technologie peut pousser cette dernière à faire de même pour rester compétitive. Par exemple, si un pâtissier utilise Instagram pour promouvoir ses produits, cela peut inciter un autre pâtissier à se digitaliser et à utiliser également cette plateforme afin de rester dans la course et de pouvoir rivaliser.

Un cadre réglementaire et un soutien gouvernemental via une stratégie nationale dédiée à la digitalisation du pays peuvent aussi bénéficier significativement aux petites et moyennes entreprises. Pour le coup, la Suisse a mis en place une stratégie, celle-ci met en avant chaque année plusieurs thèmes prioritaires. Pour 2024, les axes prioritaires incluent la cybersécurité, le cadre réglementaire de l'intelligence artificielle, et les interfaces électroniques de programmation, ou API. La stratégie s'adapte en fonction de ces thèmes. Cela montre l'engagement du gouvernement à créer un environnement propice à une transition numérique efficace pour tous les acteurs d'un pays dont les PME. *(Digitale Schweiz 2023)*

2.4 Évaluation de la digitalisation

Nous avons déjà abordé les différents facteurs qui influencent le niveau de digitalisation. À présent, nous explorerons comment quantifier et objectiver la digitalisation pour obtenir une perspective concrète et mesurable.

2.4.1 Infrastructure et technologie

2.4.1.1 Matérielle

Nous pouvons établir un ratio basé sur le nombre d'ordinateurs et de périphériques connectés par rapport au nombre total d'employés. Nous surveillons également la façon dont les données sont stockées sur un serveur de manière locale ou bien à travers le cloud. On regarde aussi comment les données sont partagées que ce soit sur des réseaux internes comme un intranet ou bien externe via internet.

2.4.1.2 Immatérielle

2.4.1.2.1 *Software*

Nous dressons un inventaire de tous les logiciels utilisés, y compris les ERP, CRM, CMS, suites bureautiques, etc. Nous vérifions la compatibilité des différents logiciels entre eux, identifions les connexions manquantes ainsi que les doublons, c'est-à-dire les logiciels qui remplissent des fonctions similaires.

2.4.1.2.2 *Formation des employés*

Il faut noter le nombre de formation continu que la PME offre à ses employés que ce soit en interne ou bien en externe. On peut faire un ratio en fonction du nombre de certification par employé en fonction du nombre d'employé total.

2.4.1.2.3 *Présence en ligne*

Nous examinons la présence en ligne de la PME sur des plateformes telles qu'Instagram et LinkedIn. Nous évaluons le nombre de followers, le nombre de publications par mois, ainsi que le nombre de visites sur le site web de l'entreprise ou sur le profil LinkedIn. Il y a aussi des outils en ligne afin de tester le référencement SEO de son site web. (Donninger 2021)

2.4.2 Processus et workflow

Le but est de référencer le nombre de processus digitalisés, on peut remplir un plan de capacités fonctionnelles (PCF) avec une légende indiquant les processus digitalisés et ceux qui ne le sont pas (*Voir annexe 1 : Exemple plan de capacités fonctionnelles*). Cela peut permettre ensuite de faire un ratio du nombre de processus digitalisés par rapport au nombre total de processus dans l'entreprise.

Sur le PCF, on distingue plusieurs zones distinguant le type de processus identifié. On retrouve :

- Les processus opérationnels, ce sont tous les processus directement liés à l'activité principale de l'entreprise
- Les processus de supports, ce sont tous les processus qui accompagnent et permettent aux processus métiers de se dérouler correctement. On retrouve les processus liés à la comptabilité, aux ressources humaines par exemple.
- Les processus de pilotages, ce sont tous les processus de management. Il y a la gestion des promotions internes par exemple.
- Les processus d'échanges, ce sont tous les processus liés avec l'extérieur. On retrouve les communications avec les clients ou les commandes avec les fournisseurs par exemple.

2.4.3 Gouvernance numérique

2.4.3.1 Sécurité

Nous vérifions si l'entreprise dispose d'une politique de sécurité et évaluons la fréquence de ses mises à jour. Nous examinons également la fréquence des formations en sécurité informatique. De plus, nous listons quels outils sont employés pour renforcer la sécurité, tels que les VPN, les gestionnaires de mots de passe, les pare-feux, les antivirus et les systèmes de sauvegarde.

2.4.3.2 Gestion des données

Nous évaluons l'existence d'une politique de protection des données au sein de l'entreprise et les mesures mises en place pour gérer le consentement des données collectées. Nous examinons également les mesures de sécurité déployées pour protéger ces informations, telles que la pseudonymisation et le chiffrement, ainsi que les procédures permettant leur modification ou suppression selon les besoins. En outre, nous nous interrogeons sur la réalisation d'audits, à la fois internes et externes, et sur la fréquence de ces audits. Enfin, nous analysons comment l'entreprise implémente les actions correctives pour donner suite aux résultats des audits.

3. Chapitre 3 : Les défis de la cybersécurité pour les PME suisses

3.1 Importance de la cybersécurité pour les PME

« Une PME suisse sur dix a déjà été victime d'une cyberattaque » (*Chavanne, Kaat 2023*). Cette statistique ne représente que les entreprises pour lesquelles les attaques ont eu l'effet escompté. En réalité, plus de 40% des cyberattaques ciblent spécifiquement les PME. (*Goareguer 2023*)

Cette vulnérabilité est souvent aggravée par la manière dont les intervenants au sein des PME perçoivent les risques. De nombreux acteurs au sein des PME considèrent que les cyberattaques sont des problèmes qui touchent uniquement les autres, ce qui les amène à ne pas se sentir personnellement concernés. Ils ont souvent tendance à penser que les questions de cybersécurité doivent être gérées par les échelons supérieurs de l'entreprise, déléguant ainsi la responsabilité à leurs supérieurs hiérarchiques. (*Koller 2022*)

Bien que les petites et moyennes entreprises puissent se sentir moins concernées ou ne semblent pas être des cibles directes pour les attaquants, elles constituent souvent une porte d'entrée vers des cibles plus importantes. Du fait de leur taille réduite et des budgets limités qu'elles peuvent allouer à la cybersécurité, il est fréquemment plus stratégique pour les cybercriminels de s'attaquer à un fournisseur ou un sous-traitant par exemple.

3.2 Les principales menaces et vulnérabilités

3.2.1 Ingénierie sociale/OSINT

3.2.1.1 Qu'est-ce que c'est l'ingénierie sociale ?

L'ingénierie sociale exploite des instincts humains fondamentaux comme la confiance, la peur ou le respect de l'autorité. Cette exploitation permet de manipuler les individus pour qu'ils révèlent des informations confidentielles ou fassent des actions compromettantes. (*Nelson 2021*)

C'est une technique très répandue pour obtenir des informations, principalement parce qu'elle requiert moins de compétences techniques et davantage d'astuce.

« Pourquoi se donner la peine de défoncer une porte quand on peut simplement demander à quelqu'un de nous remettre la clé ? » (*MacKay 2023*)

Les techniques d'ingénierie sociale continuent d'évoluer, les cyberattaquants renouvelant constamment leurs méthodes pour rester un pas en avant. Trois grandes techniques prédominent : (*NowTeam 2024*)

- Le phishing ou hameçonnage : Cette méthode consiste à imiter une entité de confiance, telle qu'une entreprise ou une administration, dans le but de soutirer des identifiants et des mots de passe à l'utilisateur.
- Le mail du président : Dans cette technique, l'attaquant se fait passer pour une figure d'autorité, comme un cadre d'entreprise, et utilise la pression psychologique pour pousser la victime à effectuer un paiement, à donner des accès sécurisés ou à envoyer des documents confidentiels.
- Utilisation comme un cheval de Troie : Ici, l'ingénierie sociale sert à diffuser des malwares via des pièces jointes infectées. Les attaquants se font passer pour des fournisseurs de services, comme des compagnies d'électricité, et envoient un fichier, souvent sous la forme d'une fausse facture en PDF, qui contient un logiciel malveillant.

3.2.1.2 Rôle de l'OSINT dans l'ingénierie sociale

L'OSINT, ou Open Source Intelligence, désigne le processus de collecte et d'analyse d'informations accessibles publiquement sur internet. Ce n'est pas considéré comme illégal puisque ces données sont librement disponibles pour tous, et théoriquement, les personnes ont consenti à leur diffusion. Les sources d'OSINT incluent diverses plateformes telles que les sites web, les publications gouvernementales, les données géospatiales et les réseaux sociaux.

Le cyberattaquant utilise ces sources d'informations publiques pour analyser sa cible, en se renseignant sur ses habitudes, ses goûts et ses intérêts. Cette analyse aide à personnaliser et affiner l'attaque. Par exemple, si la victime utilise fréquemment Uber Eats, elle ne trouvera pas suspect de recevoir des communications prétendument envoyées par Uber Eats. Cette familiarité rend l'arnaque plus crédible et augmente les chances que la victime réponde à la sollicitation frauduleuse.

3.2.2 Ransomware

Le ransomware est un type de logiciel malveillant conçu pour prendre en otage les données ou le système de la victime. Son objectif principal est de restreindre l'accès de la victime à ses propres données, puis d'exiger une rançon, souvent financière, pour leur restitution. Cependant, il est important de noter que payer la rançon ne garantit pas la récupération des données ; les cybercriminels peuvent choisir de ne pas déverrouiller les données malgré le paiement. (*Gretten 2023*) En outre, l'Office fédéral de la cybersécurité recommande de ne pas payer les rançons pour éviter d'encourager les attaquants à récidiver et aussi de financer le milieu lié à la cybercriminalité. (*DDPS 2024*)

3.2.3 DDOS

En français, on désigne cela sous le nom d'attaque par déni de service distribué (distributed denial-of-service). Ce procédé cherche à rendre un service ou un site web indisponible en le saturant de données. Pour ce faire, plusieurs ordinateurs, souvent contrôlés par des bots, simulent un grand nombre de machines différentes. Ils sollicitent simultanément le même service pour le submerger de requêtes et provoquer sa chute. (*Buckbee 2022*)

3.3 Impacts potentiels des cyberattaques sur les PME

3.3.1 Fuite de données

Lors d'une attaque par ransomware, le pirate peut simplement bloquer l'accès aux données, entraînant leur perte et potentiellement des conséquences financières pour la victime. Cependant, il est également possible que le hacker fasse une copie des données avant de les crypter, lui permettant ainsi de les exploiter ultérieurement à sa guise ou de les divulguer.

On rencontre également des hackers éthiques, souvent appelés « white hats ». Leur motivation principale n'est pas l'argent, mais plutôt la volonté de révéler des informations qu'ils considèrent importantes au nom de la justice ou de l'éthique. Ils pratiquent en théorie la divulgation responsable, c'est un processus où ils informent de manière sécurisée les personnes concernées des vulnérabilités découvertes afin de permettre leur correction avant que les détails ne soient publiquement dévoilés. Il y a en générale un délai de 90 jours avant une divulgation complète. Il est important de noter que l'éthique est subjective et peut varier d'une personne à l'autre, à l'instar du débat sur si un boucher est un assassin ou non, qui dépend de l'interprétation personnelle de chacun. Dans ce contexte, certaines PME peuvent être victimes d'attaques par ces hackers éthiques, voyant leurs données publiées sans même avoir eu la possibilité de négocier ou de payer une rançon.

3.3.2 Espionnage

Après la monétisation et la publication des données volées, l'espionnage des données devient une pratique courante. Bien que copier des informations spécifiques puisse nécessiter des ressources considérables et semble moins pertinent pour les PME, il est tout à fait possible d'espionner les données des clients, y compris leurs comportements. Cette pratique peut fournir des renseignements précieux sur les habitudes de consommation et les préférences des clients.

3.3.3 Financier

Plus de la moitié des entreprises touchées par des cyberattaques subissent des pertes financières. (*Chavanne, Kaat 2023*). Dans le cas d'un ransomware, les criminels peuvent exiger des montants importants, infligeant ainsi un préjudice financier direct à l'entreprise. Cependant, l'impact financier peut s'étendre au-delà de la rançon. Une cyberattaque peut entraîner un ralentissement significatif ou même un arrêt complet des activités de l'entreprise. Par conséquent, la PME pourrait se trouver dans l'incapacité de générer des revenus, ce qui peut rapidement conduire à des pertes économiques substantielles.

3.3.4 Image publique

Toutes les entreprises, quelle que soit leur taille, accordent une grande importance à leur réputation, ce qui représente un levier d'influence efficace. Cela explique pourquoi les PME sont particulièrement vulnérables : elles sont souvent moins aptes à relever les défis de la cybersécurité en comparaison avec des grandes organisations. (*Tesnier 2024*)

Si une PME ne parvient pas à respecter ses échéances, comme des livraisons, à cause d'une attaque par ransomware ou de DDoS, cela peut sérieusement nuire à sa réputation.

3.3.5 Légal

Chaque entreprise suisse a le devoir d'annoncer si elle a été victime d'une cyberattaque au Centre national pour la cybersécurité (NCSC). Et cela doit être fait dans les 24 heures après la détection de l'attaque. Le NCSC peut ensuite apporter son soutien à l'entreprise par le biais d'évaluation technique par exemple. Dans le cas où une entreprise ne signale pas les incidents de manière voulue par peur pour sa réputation par exemple, elle s'expose à une amende pouvant aller jusqu'à 100 000 CHF. (*Le Temps 2023*)

3.4 Méthodes d'analyse des menaces

L'analyse des menaces est une composante cruciale de la gestion des risques. Cette démarche est essentielle, car elle permet de choisir la solution la mieux adaptée pour réduire les impacts, la probabilité d'occurrence, ou les deux, que ces menaces peuvent entraîner. Elle permet également d'optimiser le budget dédié à la cybersécurité et peut fournir des arguments solides lors de la négociation d'une cyber assurance. (Forêt 2023) On parle aussi de modèle de menace ou Threat modeling en anglais. L'idée est d'en plus de les répertorier, on va les classer selon différents critères. Il existe plusieurs méthodes afin de classer les menaces.

3.4.1 Méthode STRIDE

C'est une méthode qui a été introduite il y a plus de 25 ans chez Microsoft. Malgré les années, elle reste toujours d'actualité. Celle-ci consiste à classer les menaces selon 6 grandes familles : (Jegeib 2023)

- **Spoofing**, ce sont les menaces liées à l'usurpation d'identité.
- **Tampering**, il s'agit des menaces associées à l'altération des données.
- **Repudiation**, ces menaces sont liées à des cas où une personne peut nier avoir fait certaines actions sans qu'il soit possible de le vérifier (par exemple, à cause du manque de traces ou de logs).
- **Information disclosure**, ces menaces concernent la divulgation d'informations sensibles à des individus non autorisés.
- **Denial of service**, ce sont les menaces liées au fait de rendre une ressource ou un service non disponible pour les personnes ayant droit.
- **Elevation of privilege**, il s'agit de menaces associées à l'octroi injustifié de droits ou privilèges, qui permettent alors la réalisation d'actions non autorisées.

3.4.2 Méthode TRIKE

C'est une méthode qui se concentre sur l'audit de la sécurité à partir de la gestion des risques. Le but est de fournir un niveau de risque à chaque menace qui soit acceptable pour toutes les parties prenantes, que chaque partie prenante soit au courant de chaque menace et surtout de pouvoir trouver des mitigations à chaque menace. (Allen-Addy 2023) Pour ce faire, on va devoir :

- Identifier les actifs
- Créer des diagrammes afin de voir leurs interactions
- Identifier les menaces et les risques
- Trouver des mitigations
- Valider le modèle

3.4.3 Méthode DREAD

C'est une méthode qui va permettre de classer des menaces entre-elles suivant des critères. DREAD est un acronyme où chaque lettre est un critère :

- **D**amage, on évalue l'ampleur des dégâts potentiels.
- **R**eproductibilité, détermine la facilité pour que la menace puisse être répétée.
- **E**xploitabilité, mesure la facilité avec laquelle un attaquant peut exploiter la vulnérabilité liée à la menace.
- **A**ffected utilisateur, on estime le nombre d'utilisateur ou pourcentage d'utilisateur pouvant être touché.
- **D**écouvrabilité, évalue la facilité à découvrir la menace par l'attaquant.

4. Chapitre 4 : Bonnes pratiques et mesures

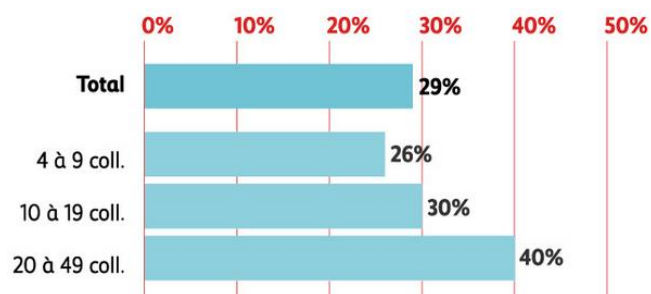
4.1 État de l'art

Des pratiques de base telles que la mise à jour fréquente des logiciels, la protection des réseaux Wi-Fi avec des mots de passe, ou encore l'utilisation de firewall sont généralement bien établies. (*Bilan.ch 2021*)

D'autres mesures relativement simples ont été mises en place, telles que l'exigence de mots de passe sécurisés (avec au moins 8 caractères, comprenant une majuscule et un symbole), ainsi que la vérification de l'origine des documents et des fichiers. (*La Mobilière 2022*)

Les prestataires informatiques occupent une position cruciale, puisque près de 30 % des PME suisses externalisent la gestion de leur cybersécurité à des fournisseurs spécialisés. (*Schäfer 2023*)

Figure 2 - Externalisation des tâches informatiques



(Schäfer 2023)

4.2 Obstacles à la mise en place de mesures de sécurités

Un des obstacles, n'est pas la mise en place tel quelle des mesures, mais de conserver une discipline stricte. Le responsable du centre de compétences Cyber Risk de La Mobilière, Simon Seebeck, a souligné lors d'une conférence que ces actions doivent aussi être actualisées et préservées. *(Chavanne, Kaat 2023)*

Un autre défi rencontré est que les PME ont tendance à négliger l'adoption de mesures de sécurité, se sentant peu concernées par ces enjeux. Selon Nicole Wettstein, « si la conscience de la menace est élevée, peu de PME se sentent concernées. Celles qui présument encore ne pas constituer une cible intéressante pour les hackers demeurent nombreuses – c'est un problème qu'il convient de traiter » *(Bilan.ch 2021)*

4.3 Lacunes et zones d'amélioration

«Il existe encore un grand potentiel dans le domaine organisationnel» *(Hölzli 2024)*

L'adoption de plans d'urgence et la réalisation d'audits de sécurité ne sont pas encore des pratiques courantes. De plus, il est fréquent que la formation des employés soit laissé pour compte, bien qu'elle soit essentielle pour combler les principales lacunes en matière de sécurité. *(Schäfer 2023)*

Il subsiste également un certain degré de négligence observé du côté technique. En effet, seulement un quart des PME effectuent régulièrement des sauvegardes de leurs données, mais bon nombre d'entre elles ne disposent pas de plan de restauration clairement établi. *(Hausmann 2022)*

4.4 Possible mitigations supplémentaires

4.4.1 Stratégies de sensibilisation axées sur l'ingénierie sociale

Le principal maillon faible et moteur des cyberattaques réside dans les erreurs humaines. Réduire ces erreurs est essentiel pour avoir un impact significatif, ce qui nécessite des formations et une sensibilisation accrue. Pour que cela soit efficace, il est essentiel que la personne formée se sente personnellement concernée.

Il serait opportun de mettre en scène la théorie. Cette dernière préconise la prudence face aux éléments sortant de la routine. Par exemple, en cas de réception d'un document ou d'une pièce jointe inhabituelle, la vigilance est de mise, en particulier pour éviter les attaques de type phishing (*MacKay 2023*). Imaginons un exemple simple pour un boucher : recevoir un courriel prétendant offrir une promotion sur une nouvelle variété de viande avec un lien suspect à cliquer.

Il est également important de rester vigilant face aux demandes inhabituelles ou urgentes, notamment dans le cadre des attaques de compromission d'e-mails commerciaux (BEC) qui ressemblent étroitement aux attaques de type « Mail du président » mentionnés précédemment (*MacKay 2023*). Par exemple, si un employé reçoit une demande urgente de paiement de la part de son supérieur hiérarchique, il est impératif de se poser des questions et de contacter directement la personne par téléphone pour confirmer l'authenticité de la demande, afin de prévenir toute tentative d'arnaque.

Il est essentiel de garder à l'esprit qu'il n'y a pas de gratuité totale ; si quelque chose semble être gratuit ou presque, alors vous êtes le produit. Si une offre semble trop belle pour être vraie, elle est très probablement suspecte. En effet, elle pourrait être une arnaque ou servir à collecter des informations pour une tentative future de social engineering (*MacKay 2023*). Prenons l'exemple d'un boucher recevant un e-mail prétendant offrir un approvisionnement gratuit en viande pour une durée limitée, mais demandant en retour des détails personnels ou bancaires. Cela pourrait être une tentative d'arnaque ou de collecte d'informations pour une utilisation ultérieure dans une attaque de phishing ou de social engineering.

Il est important de rappeler que les petites et moyennes entreprises ne sont pas toujours les principales victimes d'une attaque. Bien qu'une PME puisse sembler insignifiante à première vue pour un attaquant, elle peut néanmoins servir de point d'entrée pour atteindre une entité plus importante. Par exemple, un boucher local pourrait être utilisé comme une porte d'entrée pour cibler un fournisseur plus important. Ainsi, même les entreprises de taille modeste peuvent jouer un rôle dans les attaques visant des cibles de plus grande envergure.

4.4.2 Cas réels déjà passé en Suisse

Il peut être intéressant de mentionner que cela n'arrive pas qu'aux autres. En mentionnant par exemple des cas comme celui de la fiduciaire GRF à Morges. Où après un week-end, cette fiduciaire vaudoise, comptant 14 employés, s'est retrouvée privée de l'accès à ses systèmes par des hackers. Ces derniers ont exigé 200 000 CHF pour récupérer les données et éviter leur divulgation au public. Après avoir consulté leur prestataire informatique, la PME a découvert que les hackers bluffaient. Par conséquent, ils ont décidé de ne rien payer et ont entrepris un audit pour renforcer leur sécurité (Crevoisier et al. 2023).

4.4.3 Proposition de mesures supplémentaires

Il est possible d'obtenir une certification par des labels reconnus tels que ceux proposés par Cybersafe. Obtenir un tel label améliore non seulement la réputation cybernétique de l'entreprise auprès de ses partenaires et de son environnement, mais renforce surtout significativement sa sécurité informatique grâce aux normes imposées. Toutefois, pour un artisan, il peut être difficile en termes de temps et de coûts de mettre en œuvre de telles pratiques. Dans ce cas, une PME réticente à se certifier peut collaborer avec un prestataire IT qui respecte les standards de sécurité et qui possède des labels de qualité comme CyberSeal, garantissant sa compétence à protéger sa clientèle ou bien que le prestataire soit certifié selon la norme ISO 27001 (sécurité des systèmes d'information). (Schäfer 2023)

Des outils tel que Cybero offrent aux PME la possibilité d'accéder à des services habituellement réservés aux grandes entreprises. Parmi ces services, on trouve des audits, des formations, et des cyber-checks qui permettent initialement de dresser un état des lieux de l'entreprise. Ces analyses peuvent ensuite aider un prestataire externe à identifier les éléments principaux à protéger au sein de l'entreprise.

Une PME peut aussi opter pour une cyber-assurance pour minimiser les dommages en cas d'incident. Ce type d'assurance couvre diverses prestations, telles que la compensation pour perte de revenus due à une interruption d'activité ou bien la restauration des données. Les cyber-assurances offrent souvent des réductions aux entreprises disposant de certifications en cybersécurité, incitant ainsi les entreprises à renforcer leur responsabilité en matière de sécurité informatique. (Helvetia 2024)

4.5 Que faire en cas d'attaque ?

«La question n'est pas de savoir si on va être attaqué, mais quand.» (*Jotterand 2022*). Cette citation met en évidence la réalité inévitable des cyberattaques pour les entreprises modernes, y compris les PME suisses. Dans ce contexte, il est impératif de connaître les bonnes pratiques à adopter pour minimiser les dégâts et assurer une reprise rapide des activités.

4.5.1 Bonne pratique

Il n'existe pas de solution miracle, mais certaines bonnes pratiques permettent de stabiliser la situation et d'éviter son aggravation. Par exemple, toutes les machines doivent être débranchées du réseau et le Wi-Fi coupé pour limiter la propagation de la menace et contenir les dommages. Il est également important d'informer les responsables externes, étant donné qu'une PME dispose rarement de responsables internes spécialisés, afin de bénéficier de leur expertise et de leurs recommandations spécifiques. En outre, l'Office fédéral de la Cybersécurité ainsi que les collaborateurs doivent être informés pour gérer la situation efficacement, car une coordination et une communication claires sont essentielles pour une réponse rapide et appropriée. Isoler et sécuriser les sauvegardes va permettre de reprendre les activités efficacement en plus de ne pas aggraver la situation, car cela garantit que les données critiques sont protégées et disponibles pour la restauration. (*La Mobilière 2024*)

Il est également important de consulter les logs et les journaux d'événements pour identifier la source et l'étendue de l'incident, et aussi prendre des captures d'écran. Cela permet de documenter l'incident de manière détaillée et de fournir des informations essentielles pour les enquêtes et les réclamations. (*Fédération des Entreprises Romandes*)

4.5.2 Ce qu'il ne faut pas faire

Certaines actions sont à éviter pour ne pas aggraver la situation. L'extinction des ordinateurs peut compromettre certaines informations nécessaires à une analyse approfondie de l'incident. Le maintien des systèmes informatiques connectés au réseau et le non-coupure du Wi-Fi permettent à la menace de continuer à se propager. L'inaction et l'attente que les choses se résolvent d'elles-mêmes entraînent des dommages supplémentaires et une aggravation de la situation. Le paiement de la rançon ne garantit pas la récupération des données et encourage les cybercriminels à poursuivre leurs activités illégales. L'absence d'information par crainte des dommages à la réputation empêche une communication transparente et rapide, essentielle pour gérer la situation efficacement et minimiser les impacts. *(La Mobilière 2024)*

4.5.3 Réponse à incident

Un plan de réponse à incident est un document stratégique qui décrit les politiques, les rôles, les responsabilités, et les procédures globales pour gérer les incidents de cybersécurité dans une organisation. Il peut être complété avec un playbook qui va fournir des procédures pas à pas pour gérer des scénarios spécifiques. Il est conçu pour être utilisé en temps réel de manières concrètes.

« L'étude montre pourquoi les entreprises en Suisse sont mal préparées aux cyber-attaques et comment elles deviennent plus cyber-résilientes grâce à des méthodes de réponse aux incidents. Ainsi, seuls quatre sur dix (44,0 %) ont à portée de main des plans de réponse aux incidents qui guident l'équipe en cas d'attaque ; ils sont à peu près aussi nombreux (40,0 %) à disposer d'un playbook de réponse aux incidents. » *(Kalajdzini 2023)*

Il est vrai que pour une petite structure comme une boucherie, il semble compliqué et peu logique aux premiers abords d'avoir un plan de réponse à incident et un playbook. Cependant, un playbook centré sur des risques probables peut être facilement mis en place et s'avérer pertinent.

5. Chapitre 5 : Solution proposée : Conseils personnalisés

Ce chapitre est dédié à la présentation d'une solution innovante visant à améliorer la cybersécurité des petites et moyennes entreprises. C'est un site web interactif qui propose un questionnaire rapide et engageant. Conçu spécifiquement pour tenter de prouver que même les utilisateurs les moins familiarisés avec la cybersécurité peuvent acquérir facilement des conseils adaptés à leur situation. À travers une série de questions soigneusement élaborées, cette plateforme utilise une intelligence artificielle générative pour analyser les réponses et fournir des conseils personnalisés. Cette approche vise à offrir aux PME les outils nécessaires pour renforcer leur sécurité informatique de manière efficace et accessible.

5.1 Informations générales

Le projet est public et adopte une licence GNU car en plus de vouloir aider les PME avec une solution simple et accessible. Je veux proposer à n'importe qui d'avoir un exemple de comment intégrer de manière concrète l'api d'OpenAI. Le projet est disponible à l'adresse suivante : <https://github.com/lebretonl/2024-tb>

L'application est développée en Python (version : 3.9), elle utilise le framework FastAPI.

En raison de la nature de projet (Proof of Concept), la base de données utilisée est un fichier csv. Cela permet une mise en place simple et efficace. On retrouve les fichiers CSV dans le dossier « resultats ».

Le projet est déployé via la plateforme Back4App. Cette plateforme fournit une adresse de développement : <https://conseilcyberpmetb-zxsagubu.b4a.run/>. J'utilise le plan gratuit de cette plateforme. Cela implique quelques limites, Back4App utilise un système de « container » afin de déployer les applications. La version gratuite que j'utilise permet d'avoir 600 heures au total de déploiement, elle met également le « container » en veille après 30 minutes d'inactivité. Il faut donc le relancer manuellement si le délai est dépassé. Le projet peut aussi être déployé de manière locale à l'adresse suivante : <http://localhost:8000>. Une procédure permettant de lancer le projet local est disponible dans le fichier README.md avec le reste du code source.

Veuillez trouver ci-dessous la liste des librairies python utilisées.

Tableau 1 - Librairies python

Nom	Version
Uvicorn	0.29.0
Openai	1.27.0
FastAPI	0.0.3
Fpdf	1.7.2
Fastapi-cors	0.0.6

5.2 Utilisation de l'IA générative

On retrouve trois grandes façons d'utiliser l'IA. Il y a :

- L'IA Descriptive
- L'IA Prédictive
- L'IA Prescriptive

L'IA descriptive permet d'analyser de vastes ensembles de données pour en tirer des conclusions. Par exemple, elle peut être utilisée pour examiner les données de vente d'un magasin de vêtements afin de déterminer les meilleures périodes d'un produit spécifique.

L'IA prédictive va traiter des données qui font référence à des événements passés. Elle va tenter de trouver des patterns plus ou moins complexes. Permettant de les reconnaître dans le présent et de prédire des événements futurs. On peut l'utiliser par rapport au comportement des clients. Les résultats que l'on peut tirer servent ensuite à anticiper et produire des campagnes de marketing plus pertinentes et mieux ciblées.

L'IA prescriptive va permettre de générer des données. Ce type d'intelligence va s'entraîner sur un certain type de donnée dans le but que par la suite elle pourra générer du contenu similaire. Après qu'un modèle d'IA prescriptif ait analysé plusieurs types d'email commerciaux. Celui-ci pourra ensuite générer des nouveaux emails personnalisés. L'intelligence artificielle générative est une sous-branche de l'IA prescriptive. (Comte 2024)

Dans ce projet, j'utilise le modèle **gpt-3.5-turbo** fourni par l'API d'OpenAI. Cette API a été choisie en raison de sa simplicité d'implémentation et de sa documentation complète. OpenAI, étant un leader dans ce domaine. Il offre une certaine stabilité, garantissant que le projet peut continuer à se développer sans inquiétude.

5.3 Structure de la solution

5.3.1 Dossier « resultats »

On retrouve les fichiers CSV dans le dossier « resultats ». Il y a un premier fichier « reponses.csv » qui va accueillir les réponses du formulaire afin de les traiter par la suite. Le second fichier est le fichier « réponses_advices.csv ». Ce fichier comprend tous les conseils générés et permet de générer un résumé global.

5.3.2 Dossier « src »

Ce dossier comprend le code source, il y a deux fichiers :

- Main.py
- Utils.py

Le fichier « main » contient le code principal et est utilisé pour lancer l'application, tandis que le fichier « utils » regroupe certaines fonctions qui sont ensuite appelées dans le fichier « main ».

5.3.3 Dossier « templates »

Dans le dossier templates, nous avons les fichiers HTML qui permettent l'affichage dans un navigateur. Il y a également un fichier "base" qui définit certaines règles et propriétés pour la mise en page.

5.3.4 Dossier « static »

Ce répertoire contient les fichiers dit statiques. Cela concerne par exemple l'icône du site.

5.4 Questionnaire

Plusieurs questions sont posées, et les réponses aux questions sont intégrées dans des prompts pour être traitées par l'intelligence artificielle. Il existe deux types de prompts : les prompts systèmes et les prompts utilisateurs. Dans le prompt utilisateur, on indique ce que la personne qui interroge l'IA souhaite demander. Dans le prompt système, on définit le rôle de l'IA et on précise comment la personne qui répond au client doit se comporter.

5.4.1 Infrastructure et technologie

5.4.1.1 Matériel

Question 1

Question: Combien d'ordinateurs et de périphériques connectés utilisez-vous dans votre entreprise ?

Réponse possible : Une seule réponse possible

- 0-10
- 11-50
- 51+

Prompt utilisateur : Notre entreprise utilise {nombre} ordinateurs et périphériques connectés. Quels conseils pouvez-vous nous donner pour sécuriser ces dispositifs ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse doit contenir 3 conseils de chacun 15 mots maximum. En début de réponse, mentionnez le nombre de périphériques.

5.4.1.2 Stockage des données

Question 2

Question: Vos données sont-elles stockées localement sur des serveurs ou dans le cloud ?

Réponse possible : Une seule réponse possible

- Localement
- Dans le cloud

Prompt utilisateur: Nos données sont stockées {lieu}. Quelles mesures de sécurité devrions-nous mettre en place pour protéger ces données ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse doit contenir plusieurs conseils de chacun 15 mots maximum.

5.4.1.3 Partage des données

Question 3

Question: Comment les données sont-elles partagées au sein de votre entreprise?

Réponse possible : Une seule réponse possible

- Réseaux interne / Intranet
- Réseaux externe / Internet
- Les deux / Interne et Externe

Prompt utilisateur :

- Si mixte : Nous partageons nos données via des réseaux internes et externes. Comment pouvons-nous sécuriser ce partage de données ?
- Sinon : Nous partageons nos données via un réseau {type}. Comment pouvons-nous sécuriser ce partage de données ?

Prompt système :

- Si mixte : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse doit contenir 4 conseils de chacun 15 mots maximum.
- Sinon : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse doit contenir 2 conseils de chacun 15 mots maximum.

5.4.2 Logiciels

Question 4

Question: Quels types de logiciels utilisez-vous pour la gestion de votre entreprise?

Réponses possibles : Plusieurs choix sont possibles

- CMS / Site internet
- Logiciel de comptabilité (Crésus, Bexio...)
- CRM (Hubspot, Salesforce), ERP (SAP, Abacus ...)
- Aucun logiciel utilisé
- Zone de texte libre.

Prompt utilisateur: Nous utilisons les logiciels suivants pour la gestion de notre entreprise : {ERP, CRM, CMS, etc.}. Quels sont les meilleures pratiques pour maintenir ces logiciels sécurisés ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse doit contenir 2 conseils de 15 mots maximums par type de logiciel indiqué

5.4.3 Formation des employés

Question 5

Question: Offrez-vous des formations et/ou des séances de sensibilisations à la cybersécurité à vos employés ? Si oui, à quelle fréquence ?

Réponse possible : Une seule réponse possible

- Non
- Une seule fois
- Tous les 6 mois
- Une fois par an

Prompt utilisateur:

- Si non : Nous n'offrons pas des formations en cybersécurité à nos employés.
- Si une seule fois : Nous avons offert des formations en cybersécurité à nos employés une seule fois depuis leur début
- Si tous les 6 mois : Nous offrons des formations en cybersécurité à nos employés tous les 6 mois
- Si tous les ans : Nous offrons des formations en cybersécurité à nos employés tous les ans

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Sensibilise l'utilisateur sur l'importance de la formation en cybersécurité par rapport à son message. Fournis 1 conseil de manière concise (15 mots maximums et une notion de temps)

5.4.4 Présence en ligne

Question 6

Question: Quels sont les réseaux sociaux que vous utilisez dans un cadre professionnel ?

Réponse possible : Plusieurs réponses possible

- Aucun
- Instagram
- LinkedIn
- Facebook
- X
- Autre

Prompt utilisateur :

- Si Aucun : Nous n'utilisons pas les réseaux sociaux dans un cadre professionnel. Comment puis-je m'y préparer si jamais ?
- Sinon: Nous avons une présence active sur {liste}. Quels sont les risques que je peux rencontrer sur chaque réseau cité ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Sensibilisez également l'utilisateur sur le social engineering en lui donnant un exemple par réseaux cité s'il y en a.

5.4.5 Sécurité des systèmes

5.4.5.1 Outils

Question 7

Question: Quels outils de sécurité utilisez-vous ?

Réponse possible : Plusieurs réponses possible

- Aucun
- Antivirus
- Pare-feux
- VPN
- Gestionnaire de mot de passe
- Système de sauvegarde

Prompt utilisateur:

- Si aucun : Nous n'utilisons pas les outils de sécurités suivants : Antivirus, pare-feu, VPN, gestionnaire de mot de passe et système de sauvegarde. Quels outils me conseilles-tu en priorité ?
- Sinon : Nous utilisons les outils suivants : {liste}. Quels autres outils parmi les suivants : Antivirus, pare-feu, VPN, gestionnaire de mot de passe et système de sauvegarde devrions-nous considérer en priorité ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Pour chaque réponse, celle-ci doit être concise et comporter 15 mots maximums. Ajoute également pourquoi les outils conseillés sont prioritaires.

5.4.5.2 Réseaux wifi

Question 8

Question: Comment votre réseau wifi est-il accessible ?

Réponse possible : Une réponse possible

- Pas de mot passe
- Mot de passe simple (exemple : 123456789)
- Mot de passe moyen (exemple : Entreprise12)
- Mot de passe élevé (exemple : Mg7@Lkf232-!)

Prompt utilisateur:

Afin de sécuriser notre réseau wifi nous utilisons {typemdp}. Est-ce que cela est adapté ?

Prompt système :

- Si mot de passe élevé : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Si le niveau de sécurité est adapté, explique brièvement pourquoi une passphrase est mieux (plus facile à retenir et/ou transmettre à un client par exemple). 45 mots maximums
- Sinon : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Si le niveau de sécurité n'est pas adapté, explique brièvement le concept de passphrase avec un exemple. 45 mots maximums. Ajoute également les risques d'un réseau wifi mal sécurisé. (20 mots maximums).

5.4.6 Réactions en cas d'attaque

Question 9

Question : Quelles sont les actions que vous avez entrepris après une cyberattaque ?
(Dans le cas où vous n'avez pas subi de cyber attaque, veuillez répondre comme si cela l'était)

Réponse possible : Plusieurs réponses possible

- Vérifier les logs
- Débrancher les machines
- Contacter son prestataire informatique
- Couper le wifi
- Contacter l'Office fédérale de la cybersécurité
- Isoler les sauvegardes
- Conservation des preuves via des Screenshot

Prompt utilisateur: Voici les actions que j'ai entrepris à la suite d'une cyberattaque : {actions}. Quelles actions pourrais-je ajouter afin d'être plus efficace ?

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. La réponse fournit doit faire 50 mots maximum. Ajoute une explication supplémentaire concise (30 mots maximum) sur l'utilité et l'importance d'un plan d'urgence en cas de cyberattaque.

5.4.7 Cas concret

Question 10

Question : Quel est votre domaine d'activité ?

Prompt utilisateur : J'ai une PME dans le domaine {domaine}. Donne-moi des exemples d'attaques qui se sont déjà passée avec des entreprises similaires.

Prompt système : Vous êtes un consultant en cybersécurité expérimenté. Vous devez répondre à la question de l'utilisateur. Fournissez une réponse en français. Donne 3 exemples concrets de 20 mots chacun.

5.5 Résultat

Lors du clic sur le bouton « Télécharger les conseils en PDF ». Cela génère un PDF. Les conseils sont écrits dans ce PDF. Le document contenant les conseils peut se récupérer par l'utilisateur dans son dossier « Téléchargement ».

Un exemple de résultat est disponible dans l'annexe 3. La solution a été testée concrètement par trois responsables de PME genevoises. Chaque PDF contenant les conseils est disponible dans le dossier « resultats », accessible via GitHub.

5.5.1 Remarques personnelles

Les résultats obtenus peuvent être parfois discutable car les conseils varient lorsque les mêmes inputs sont fournis. Des utilisateurs différents pourraient recevoir des conseils divergents pour des situations identiques. Cela implique une nécessité d'améliorer les manières dont les appels à l'API d'OpenAI sont effectués. Notamment améliorer les prompts système et utilisateur.

Une autre observation notable est la présence de nombreuses répétitions dans les conseils fournis au sein des documents PDF générés. Cette redondance peut rendre les documents moins lisibles et réduire la valeur perçue des recommandations.

Le questionnaire doit être amélioré, lors des tests effectués avec les responsables de PME, j'ai constaté que certaines questions manquaient de réponses adaptées. Par exemple, pour les questions concernant la sécurisation du wifi, il manquait une option pour les entreprises n'ayant pas de réseau wifi disponible. De plus, pour le lieu de stockage des données, l'utilisateur peut actuellement indiquer uniquement s'il stocke localement ou dans le cloud. Cependant, une entreprise a signalé qu'elle stockait une partie de ses données dans le cloud et une autre partie localement.

5.5.2 Analyse feedback utilisateur

À la fin du questionnaire, après avoir récupéré ses conseils personnalisés sous format PDF, l'utilisateur peut laisser un avis. Il y a un bouton qui redirige vers un formulaire google vers cette adresse :

https://docs.google.com/forms/d/1e_wSNGj8NRx-5LA5GjxdKbGIWyuXqMlj3psEbjOhKlw

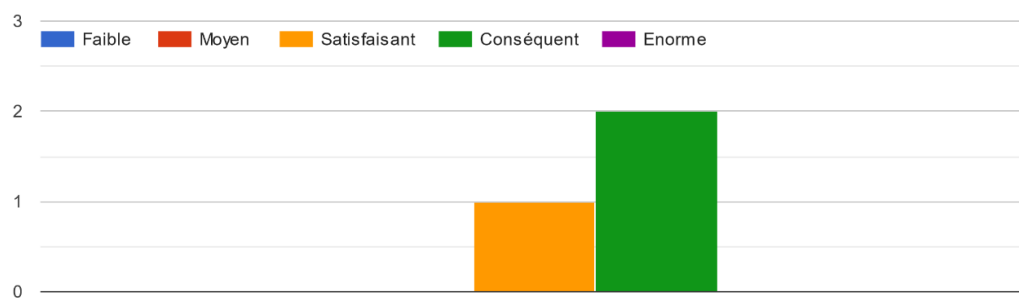
L'utilisateur peut évaluer son expérience en examinant la quantité de conseils fournis, leur pertinence et le nombre qu'il pourrait en mettre en œuvre.

5.5.2.1 Résultat formulaire

5.5.2.1.1 Quantité des conseils fournis

Figure 3 - Réponse formulaire, question 1

Comment évaluez-vous la quantité des conseils fournis ?



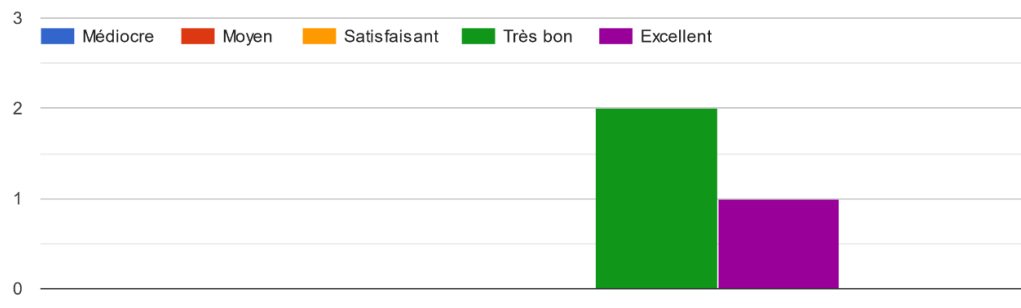
La figure 3 montre les évaluations des utilisateurs concernant la quantité de conseils fournis. Les utilisateurs ont classé les conseils dans différentes catégories : Faible, Moyen, Satisfaisant, Conséquent et Enorme

La majorité des utilisateurs (2 sur 3) estiment que la quantité de conseils est conséquente, ce qui peut indiquer une richesse en informations fournies. Un utilisateur trouve la quantité satisfaisante, ce qui montre que, pour certains, le volume est bien équilibré. L'absence de réponses dans les catégories : faible, moyen et énorme indique que les utilisateurs ne ressentent ni un manque ni un excès significatif de conseils.

5.5.2.1.2 Pertinence des conseils fournis

Figure 4 - Réponse formulaire, question 2

Comment évaluez-vous la pertinence des conseils fournis ?



La figure 4 présente les évaluations des utilisateurs concernant la pertinence des conseils fournis. Les utilisateurs ont classé les conseils dans les catégories suivantes : Médiocre, Moyen, Satisfaisant, Très bon, et Excellent.

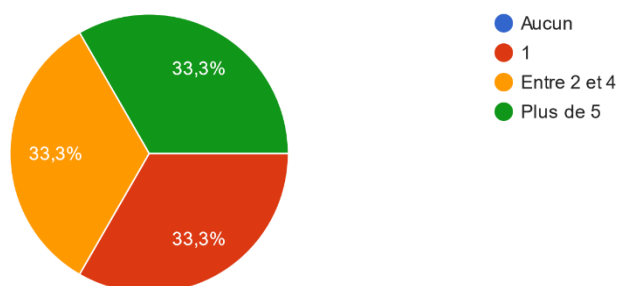
Deux tiers des utilisateurs considèrent les conseils comme très bons, soulignant ainsi une perception positive et une qualité élevée des recommandations fournies. Un tiers des utilisateurs trouve les conseils excellents, ce qui indique que, pour certains, les conseils dépassent les attentes en termes de pertinence. L'absence de réponses dans les catégories : médiocre, moyen et satisfaisant montre que les utilisateurs ne perçoivent pas de défauts ni de manque de pertinence dans les conseils fournis.

5.5.2.1.3 Application des conseils fournis

Figure 5 - Réponse formulaire, question 3

Parmi les conseils fournis, combien d'entre eux pourriez-vous mettre en œuvre ?

3 réponses



La figure 5 démontre la répartition des réponses des utilisateurs concernant le nombre de conseils qu'ils pourraient mettre en œuvre parmi ceux qui leur ont été fournis. L'utilisateur a pu choisir s'il intégrait aucun conseil, un conseil, entre deux et quatre conseils ou plus de cinq conseils.

Les résultats indiquent que les utilisateurs sont prêts à appliquer au moins un conseil. La répartition au sein des catégories est équivalente, avec un tiers des utilisateurs dans chacune.

5.5.2.1.4 Interprétation globale des résultats

Quand on met en lien la figure 3 concernant la quantité de conseils qui est jugé entre satisfaisante et conséquente avec la figure 5 qui concernent le nombre de conseil applicable, on constate un écart significatif entre la quantité (plus d'une vingtaine ainsi qu'un résumé) et leur mise en œuvre. On pourrait penser que les conseils ne sont pas pertinents ou adaptés, mais la figure 4 réfute cette hypothèse. Il serait plutôt nécessaire de rendre les conseils fournis plus applicables et peut-être de réduire légèrement la quantité de conseils générés.

6. Chapitre 6 : Conclusion

6.1 Digitalisation

La digitalisation des PME suisses est une étape primordiale pour leur compétitivité et leur survie dans un environnement économique de plus en plus numérique. Les PME jouent un rôle essentiel dans l'économie suisse, représentant une majorité des emplois et des entreprises du pays. Cependant, l'adoption de la digitalisation reste variable, influencée par des facteurs internes comme le conservatisme et les ressources limitées, et des facteurs externes tels que la concurrence et les réglementations gouvernementales. Malgré ces défis, il est impératif pour les PME de continuer à investir dans des technologies numériques et de former leur personnel pour rester pertinentes et efficaces. Les entreprises doivent également être objectives quant à leur niveau de digitalisation. Bien que de nombreuses méthodes existent pour évaluer le niveau de digitalisation d'une entreprise, celles-ci peuvent varier considérablement d'une entreprise à l'autre et d'un pays à l'autre. Il existe des normes pour la digitalisation des données sensibles, telles que la norme 21 CFR Part 11 (*Gxpmanager 2023*), mais aucune pour évaluer le niveau de digitalisation global. Pourquoi ne pas instaurer un standard d'évaluation pour remédier à cela ?

6.2 Cybersécurité

La cybersécurité est un enjeu majeur pour les PME, qui sont fréquemment ciblées par des cyberattaques en raison de leurs ressources limitées pour se défendre. Les principales menaces incluent l'ingénierie sociale, les ransomwares et les attaques DDoS, chacune pouvant avoir des impacts dévastateurs sur les finances, la réputation et l'aspect légal des entreprises. La sensibilisation aux menaces et l'adoption de bonnes pratiques en matière de cybersécurité sont essentielles pour protéger les actifs numériques des PME. L'utilisation de méthodes d'analyse des menaces, comme STRIDE, TRIKE et DREAD, peut aider à évaluer et à atténuer les risques de manière efficace même si ces méthodes peuvent paraître contre intuitives pour une entreprise peu digitalisée.

6.3 Bonnes pratiques

Les PME ont actuellement adopté quelques pratiques de cybersécurité tel que l'utilisation de pare-feu, la protection des réseaux wifi, l'utilisation de mots de passe sécurisés ou bien le contrôle de l'origine des documents reçus par email. Les obstacles à ces mesures peuvent inclure un manque de sensibilisation, des ressources limitées et des attitudes conservatrices. Il est important d'identifier les lacunes dans les pratiques de sécurité actuelles et de proposer des améliorations, telles que des formations, l'élaboration de plan d'urgence et d'audit ou bien de la mise en place de sauvegardes fréquentes.

Le maillon faible au sein de la cybersécurité d'une entreprise étant principalement l'humain, l'amélioration principale doit se concentrer sur comment changer des mauvaises habitudes. Cela rejoint un des obstacles qui est le manque de ressources disponible attribuable à la cybersécurité. Il est moins coûteux et plus efficace de former son personnel que de déboursier des grandes sommes dans du matériel et dans un domaine technique qui peut parfois dépasser le principal intéressé.

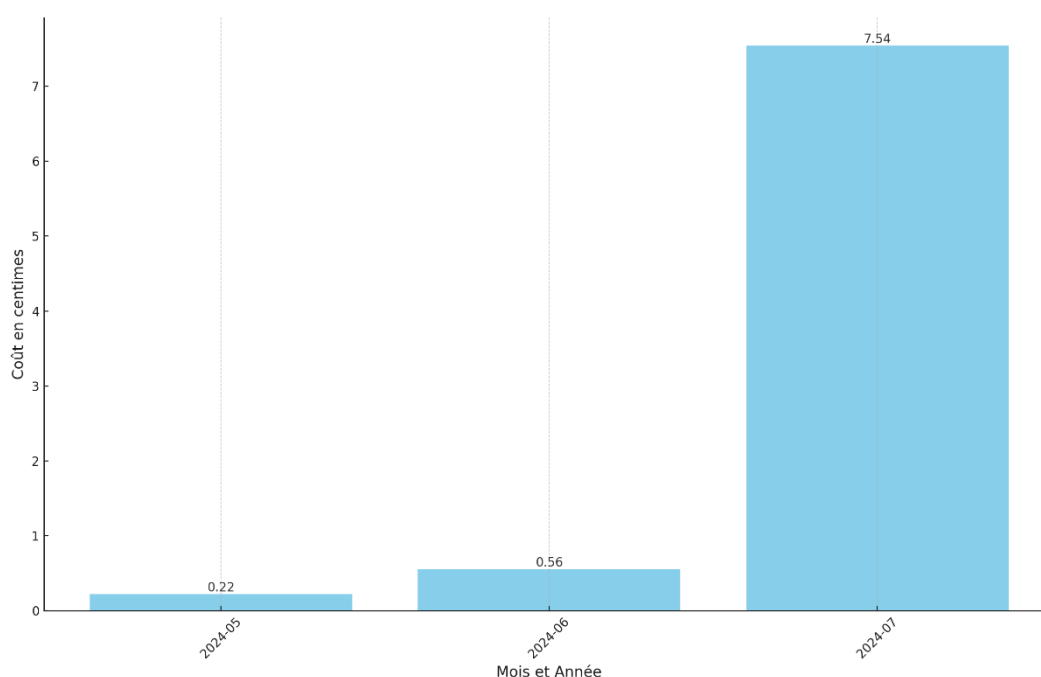
6.4 Solution

La solution proposée dans ce travail de Bachelor offre des conseils personnalisés, pertinents et applicables. Ils sont basés sur la situation professionnelle des utilisateurs concernés.

Actuellement, on retrouve comme concurrent des entreprises comme Cyber'up, qui propose en plus de conseils personnalisés des tests d'intrusions. La différence avec la solution que je propose est premièrement par rapport au coût. Cyber'up facture entre 7080 CHF et 13080 CHF l'année (*Cyber'up 2022*).

La valeur ajoutée de mon application réside dans son coût. Pour l'ensemble du projet, les appels à l'API d'OpenAI ont coûté moins de 10 centimes. Cela inclut la phase de développement et la phase de test avec les 3 entreprises.

Figure 6 - Coût mensuel en centimes



Un consultant en cybersécurité est rémunéré aux alentours de 66 CHF par heure (*Talent.ch* 2024). Par expérience personnelle, on peut multiplier ce taux horaire par 6 pour déterminer le taux à facturer au client, ce qui correspond à environ 396 CHF par heure. Lors des tests de mon application avec des entreprises, l'entretien avec le client durait environ 20 minutes comprenant la réponse au formulaire, la génération des conseils, ainsi que leur lecture. Ainsi, en considérant que l'utilisation de l'application équivaut à une consultation de 20 minutes avec un consultant, le coût estimé de cette consultation serait de 132 CHF. Cela fournit une base pour déterminer le tarif potentiel à facturer par utilisation à un client.

Une autre valeur ajoutée de ma solution réside dans sa facilité de mise en œuvre et sa courte durée. L'incertitude et le temps requis peuvent constituer des freins pour ceux qui ne perçoivent pas immédiatement l'intérêt de la cybersécurité.

6.4.1 Limite de la solution

Le modèle OpenAI étant payant, il est compliqué de publier la solution en ligne et de la rendre libre d'accès en raison des coûts élevés associés à la facturation par token.

Les conseils générés contiennent de nombreuses redondances, ce qui peut compliquer leur lecture et leur assimilation.

La phase de test de l'application a été compliquée avec le projet déployé en local.

6.4.2 Perspective de la solution

Le déploiement de la solution sur le web faciliterait la phase de test, offrant une expérience utilisateur plus réelle et concrète. Un système de connexion avec un couple identifiant/mot de passe pourrait être mis en place pour réguler les accès à l'application, ceci permettrait d'éviter une surfacturation et de contrôler l'utilisation de la plateforme.

Il serait pertinent d'inclure des sources étayer les conseils, comme par exemple le nom d'un gestionnaire de mots de passe existant, afin de renforcer la pertinence et l'applicabilité des recommandations.

Dans un premier temps, il faudrait améliorer les prompts systèmes et les prompts utilisateurs. Cela permettrait d'avoir moins de redondance au sein d'un même PDF, mais aussi d'éviter une variabilité des conseils fournis pour différents utilisateurs ayant des données similaires lors du remplissage du formulaire. Pour cela, on pourrait se focaliser sur la gestion de certains paramètres des prompts tels que la température qui contrôle la créativité de la réponse. On peut également ajuster le contexte au sein des prompts systèmes, actuellement on précise un certain nombre de conseils, on pourrait réduire ces nombres afin d'éviter la redondance. Dans un second temps, on pourrait changer le type d'appel d'API. Actuellement, nous utilisons la fonctionnalité de complétion de l'API OpenAI pour fournir des conseils personnalisés. La complétion permet de générer du texte par rapport à un prompt donné. Cependant, il serait avantageux d'explorer l'utilisation du mode assistant, qui permet d'intégrer des documents spécifiques à l'entreprise, tels que des politiques de sécurité interne existantes. Le mode assistant est une fonctionnalité plus avancée qui permet d'avoir une interaction plus structurée en incluant des documents de référence par exemples. Cette approche offrirait l'opportunité d'avoir des conseils encore plus personnalisés.

L'intégration d'un modèle d'intelligence artificielle local permettrait d'entraîner l'IA de manière plus pertinente, en utilisant des données spécifiques et contrôlées comme des politiques de sécurités suisses existantes ou bien des recommandations cantonales/fédérales. De plus, cette approche garantirait une meilleure sécurité en évitant l'envoi des données à des tiers, permettant ainsi de poser des questions plus privées en toute confidentialité.

La mise en page actuelle des documents PDF générés n'est pas optimale. Une révision est nécessaire, on pourrait commencer par un état général, suivi d'un résumé, et continuer avec des conseils d'habitudes pour ensuite finir par des conseils plus techniques. L'objectif serait de progresser du général au spécifique, permettant aux lecteurs moins compétents techniquement de s'arrêter à un niveau de détail qui leur correspond. On pourrait également imaginer une structure de document dynamique où l'utilisateur peut choisir à la fin du questionnaire par exemple s'il préfère une liste de conseils ou du texte ou bien s'il souhaite des conseils d'habitudes ou techniques.

6.5 Avis personnel

Je suis satisfait des résultats obtenus. Le formulaire indique que les utilisateurs pourraient intégrer plusieurs conseils dans leur quotidien, ce qui démontre un réel besoin et un intérêt. Je suis motivé à continuer de développer cette application dans le futur ou à travailler sur des projets similaires. Il existe de nombreuses voies d'amélioration, comme mentionné précédemment. Le sujet de la cybersécurité est à la fois intéressant et pertinent, touchant tout le monde, ce qui renforce l'importance de ce projet. Au cours de ce projet, j'ai appris de nombreuses choses et j'ai pu appliquer des notions vues en cours, tant sur le plan théorique que technique. Cela m'a permis de renforcer mes compétences et d'approfondir ma compréhension de la cybersécurité.

Bibliographie

ALLEN-ADDY, Claire, 2023. Threat Modeling Methodology: TRIKE. [en ligne]. 29 septembre 2023. Disponible à l'adresse : <https://www.iriusrisk.com/resources-blog/trike-threat-modeling-methodologies> [consulté le 26 avril 2024].

BILAN.CH, 2021. Cyber-criminalité – Trop de PME se protègent mal contre les cyberattaques (étude). *Bilan* [en ligne]. 18 novembre 2021. Disponible à l'adresse : <https://www.bilan.ch/story/trop-de-pme-se-protagent-mal-contre-les-cyberattaques-etude-828527705322> [consulté le 3 mai 2024].

BUCKBEE, Michael, 2022. Qu'est-ce qu'une attaque par déni de service distribué (DDoS) ? [en ligne]. 11 février 2022. Disponible à l'adresse : <https://www.varonis.com/fr/blog/attaque-par-deni-de-service-distribue-ddos> [consulté le 26 avril 2024].

CHAVANNE, Yannick et KAAT, Coen, 2023. Les PME suisses sont toujours à la traîne en matière de sécurité IT. [en ligne]. 21 septembre 2023. Disponible à l'adresse : <https://www.ictjournal.ch/etudes/2023-09-21/les-pme-suisses-sont-toujours-a-la-traine-en-matiere-de-securite-it> [consulté le 7 mars 2024].

COMTE, Nathan, 2024. Quels sont les différents types d'IA ? *Digitad* [en ligne]. 6 mai 2024. Disponible à l'adresse : <https://digitad.fr/les-differents-types-d-ia/> [consulté le 10 juillet 2024].

CONFÉDÉRATION SUISSE, 2024a. Faits et chiffres sur les PME en Suisse. [en ligne]. 3 janvier 2024. Disponible à l'adresse : <https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/politique-pme-faits-et-chiffres.html> [consulté le 7 mars 2024].

CONFÉDÉRATION SUISSE, 2024b. Portrait du Secrétariat d'État à l'économie. [en ligne]. 2 février 2024. Disponible à l'adresse : https://www.seco.admin.ch/seco/fr/home/seco/seco_portraet.html [consulté le 15 avril 2024].

CONFÉDÉRATION SUISSE, 2024c. Chiffres sur les PME: entreprises et emplois. [en ligne]. 4 janvier 2024. Disponible à l'adresse : <https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/politique-pme-faits-et-chiffres/chiffres-sur-les-pme/entreprises-et-emplois.html> [consulté le 15 avril 2024].

CREVOISIER, Julien et al., 2023. Cyberattaques: trois entreprises témoignent. *pme* [en ligne]. 22 mai 2023. Disponible à l'adresse : <https://www.pme.ch/dossiers-et-hors-series/2023/05/22/cyberattaques-trois-entreprises-temoignent-604326> [consulté le 6 mai 2024].

CSEM, 2023. Ne pas rater sa numérisation - Le Temps. [en ligne]. 20 novembre 2023. Disponible à l'adresse : <https://www.letemps.ch/suisse/ne-pas-rater-sa-numerisation> [consulté le 15 avril 2024].

CYBER'UP, 2022. Nos offres cybersécurité pour sécuriser votre entreprise et votre site web. [en ligne]. 2022. Disponible à l'adresse : <https://www.cyberup.ch/nos-offres-cybersecurite/> [consulté le 15 juillet 2024].

DDPS, Département fédéral de la défense, de la protection de la population et des sports, 2024. Rançongiciels – que faire? [en ligne]. 1 janvier 2024. Disponible à l'adresse : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html> [consulté le 3 mai 2024].

DIGITALE SCHWEIZ, 2023. Stratégie Suisse numérique 2024 - YouTube. [en ligne]. 19 décembre 2023. Disponible à l'adresse : <https://www.youtube.com/watch?v=1dVfSeROxhc&t=69s> [consulté le 15 avril 2024].

DONNINGER, Stéphane, 2021. Comment savoir si son site est bien référencé ? [en ligne]. 16 février 2021. Disponible à l'adresse : <https://www.agence-copernic.fr/blog/referencement-site> [consulté le 17 avril 2024].

FÉDÉRATION DES ENTREPRISES ROMANDES. Que faire en cas de cyberattaque ? - FER Genève. [en ligne]. Disponible à l'adresse : <https://www.fer-ge.ch/que-faire-en-cas-de-cyberattaque-hacking> [consulté le 2 juillet 2024].

FORÊT, Christophe, 2023. Analyse des risques : quelle méthode pour les risques cyber ? [en ligne]. 30 mai 2023. Disponible à l'adresse : <https://www.c-risk.com/fr/blog/analyse-des-risques> [consulté le 26 avril 2024].

GOAREGUER, Gaëlle, 2023. Cibles de cyberattaques – Votre PME est-elle prête? [en ligne]. 16 mars 2023. Disponible à l'adresse : <https://www.bdo.ch/fr-ch/publications/articles/nl/cibles-de-cyberattaques-votre-pme-est-elle-prete> [consulté le 25 avril 2024].

GRETTE, Justine, 2023. Qu'est-ce qu'un ransomware ? *Mailinblack* [en ligne]. 24 octobre 2023. Disponible à l'adresse : <https://www.mailinblack.com/ressources/glossaire/quest-ce-quun-ransomware/> [consulté le 25 avril 2024].

GXPManager, 2023. Digitalisation et mise en conformité avec la norme 21 CFR Part 11. *GxpManager - Application Builder* [en ligne]. 10 mars 2023. Disponible à l'adresse : <https://gxpmanager.com/la-digitalisation-des-donnees-en-conformite-avec-la-norme-21-cfr-part-11-de-la-fda> [consulté le 18 juillet 2024].

HAUSMANN, Roger, 2022. Les PME ne prennent pas suffisamment au sérieux la cybersécurité. *Swisscom B2B Mag* [en ligne]. 6 juillet 2022. Disponible à l'adresse : <https://www.swisscom.ch/fr/b2bmag/securite/pme-cybersecurite-protection/> [consulté le 3 mai 2024].

HELVETIA, 2024. Cyber-assurance. *Helvetia Assurances* [en ligne]. 2024. Disponible à l'adresse : <https://www.helvetia.com/ch/web/fr/entreprises/assurances/cyber/cyber-assurance.html> [consulté le 3 mai 2024].

HÖLZLI, Andreas, 2024. Avis d'expert: bien que les PME se protègent mieux des pirates informatiques, des lacunes subsistent | Swiss Venture Club. [en ligne]. mai 2024. Disponible à l'adresse : <https://svc.swiss/fr/avis-dexpert-bien-que-les-pme-se-protagent-mieux-des-pirates-informatiques-des-lacunes-subsistent-1> [consulté le 3 mai 2024].

JEGEIB, 2023. Menaces - Outil Microsoft de modélisation des menaces - Azure. [en ligne]. 1 juin 2023. Disponible à l'adresse : <https://learn.microsoft.com/fr-fr/azure/security/develop/threat-modeling-tool-threats> [consulté le 26 avril 2024].

JOTTERAND, Raphaël, 2022. Cybersécurité: «La question n'est pas de savoir si on va être attaqué, mais quand» - Le Temps. [en ligne]. 11 octobre 2022. Disponible à l'adresse : <https://www.letemps.ch/suisse/valais/cybersecurite-question-nest-savoir-on-va-attaque> [consulté le 6 mai 2024].

KALAJDZINI, Adelisa, 2023. Plans de réponse aux incidents : la Suisse est-elle « cyber-résiliente » ? *Organisateur* [en ligne]. 25 septembre 2023. Disponible à l'adresse : <https://www.organisator.ch/fr/excellence-operationnelle/2023-09-25/incident-response-plaene-ist-schweiz-cyberresilient/> [consulté le 2 juillet 2024].

KOLLER, Rodolphe, 2022. Sensibles aux cyberattaques, les PME suisses ne s'y estiment guère exposées directement. [en ligne]. 29 juin 2022. Disponible à l'adresse :

<https://www.ictjournal.ch/etudes/2022-06-29/sensibles-aux-cyberattaques-les-pme-suissees-ne-sy-estiment-guere-exposees> [consulté le 24 avril 2024].

LA MOBILIÈRE, 2022. (1) Les PME se protègent toujours aussi peu | LinkedIn. [en ligne]. 28 juin 2022. Disponible à l'adresse : <https://www.linkedin.com/pulse/les-pme-se-prot%C3%A8gent-toujours-aussi-peu-die-mobilier/> [consulté le 6 mai 2024].

LA MOBILIÈRE, 2024. Que faire en cas de cyberattaque? [en ligne]. 2024. Disponible à l'adresse : <https://www.mobiliere.ch/guide/que-faire-en-cas-de-cyberattaque> [consulté le 2 juillet 2024].

LE MONDE ÉCONOMIQUE, 2019. Les PME suisses bien armées pour la numérisation, mais... *Le Monde Économique* [en ligne]. 21 mars 2019. Disponible à l'adresse : <https://www.monde-economique.ch/les-pme-suissees-bien-armees-pour-la-numerisation-mais/> [consulté le 15 avril 2024].

LE TEMPS, 2023. Jusqu'à 100 000 francs d'amende si une cyberattaque n'est pas signalée - Le Temps. [en ligne]. 21 septembre 2023. Disponible à l'adresse : <https://www.letemps.ch/cyber/jusqu-a-100-000-francs-d-amende-si-une-cyberattaque-n-est-pas-signalee> [consulté le 26 avril 2024].

MACKAY, James, 2023. Social engineering attack | Signes d'attaque par ingénierie sociale. *MetaCompliance* [en ligne]. 2 juin 2023. Disponible à l'adresse : <https://www.metacompliance.fr/blog-cybersecurite/phishing-et-ransomware/social-engineering-attack-signe-attaque-ingenierie-sociale> [consulté le 25 avril 2024].

NELSON, Brittany, 2021. Qu'est-ce que l'ingénierie sociale et êtes-vous menacé ? *Qu'est-ce que l'ingénierie sociale et êtes-vous menacé ?* [en ligne]. 20 janvier 2021. Disponible à l'adresse : <https://www.avg.com/fr/signal/what-is-social-engineering> [consulté le 25 avril 2024].

NOWTEAM, 2024. Ingénierie Sociale : Sécurité et Risques Employés. *NowTeam, Spécialiste de l'infogérance et maintenance informatique* [en ligne]. 22 janvier 2024. Disponible à l'adresse : <https://www.nowteam.net/ingenierie-sociale-employes-principale-faille-de-securite/> [consulté le 25 avril 2024].

RETAIL, Univers, 2022. L'industrie 4.0. *Univers Retail* [en ligne]. 22 avril 2022. Disponible à l'adresse : <https://www.universretail.com/lindustrie-4-0/> [consulté le 15 avril 2024].

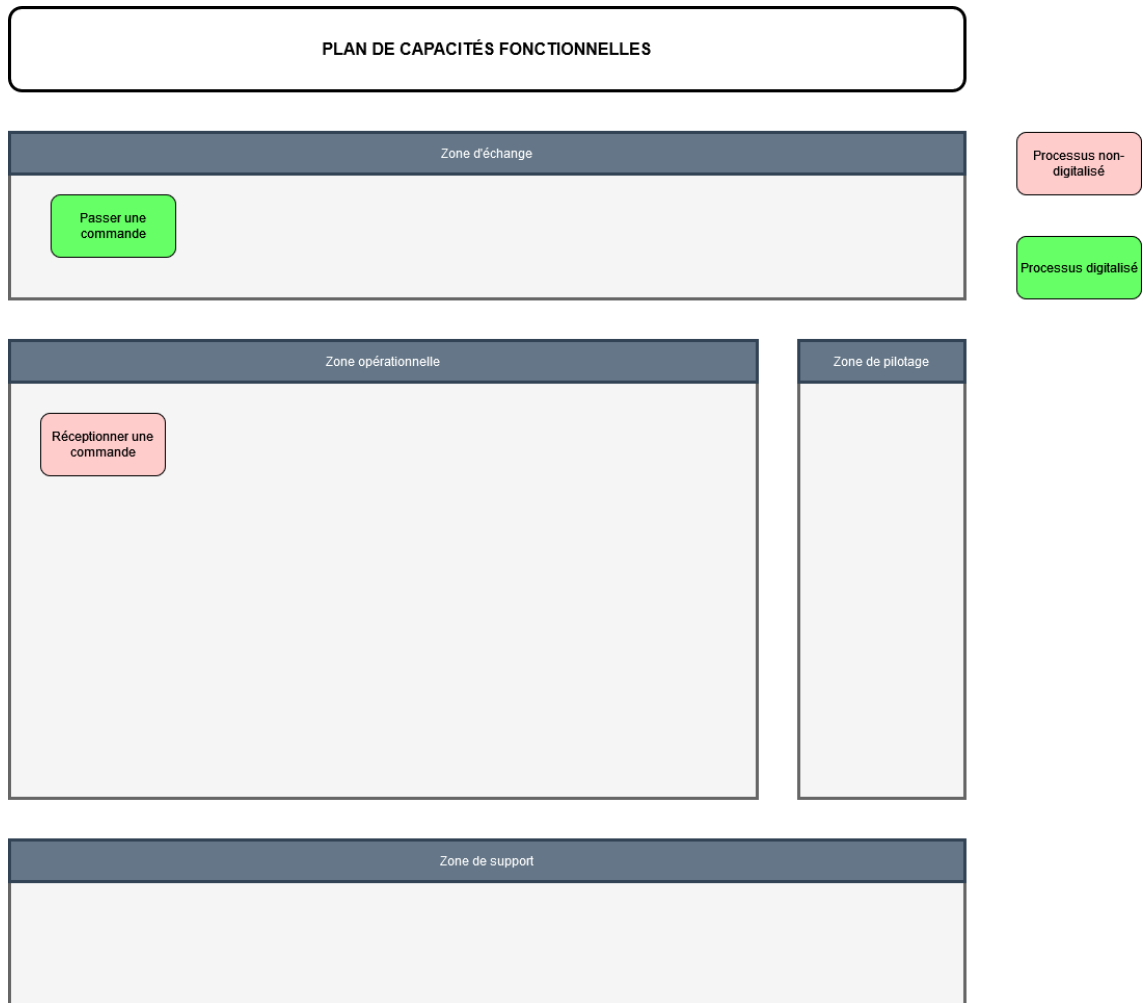
SCHÄFER, Martina, 2023. Cybersécurité: les PME ont intérêt à faire appel à un prestataire informatique. [en ligne]. 13 mars 2023. Disponible à l'adresse : <https://www.ictjournal.ch/articles/2023-03-13/cybersecurite-les-pme-ont-interet-a-faire-appel-a-un-prestataire-informatique> [consulté le 3 mai 2024].

TALENT.CH, 2024. Salaire Cyber Security, Suisse - Salaire Moyen. *Talent.com* [en ligne]. 2024. Disponible à l'adresse : <https://ch.talent.com/fr/salary> [consulté le 15 juillet 2024].

TESNIER, Grégory, 2024. Les PME romandes, cibles privilégiées des cyberattaques. *Entreprise Romande* [en ligne]. 30 janvier 2024. Disponible à l'adresse : <https://www.entrepriseromande.ch/web/er/w/les-pme-romandes-cibles-privilegiees-des-cyberattaques> [consulté le 26 avril 2024].

WAGNER, Steven et KINDLE, Fabian, 2020. Les artisans suisses voient la numérisation comme une opportunité. [en ligne]. 10 août 2020. Disponible à l'adresse : <https://www.ictjournal.ch/etudes/2020-08-10/les-artisans-suisse-voient-la-numerisation-comme-une-opportunite> [consulté le 15 avril 2024].

Annexe 1 : Exemple plan de capacités fonctionnelles



Annexe 2 : Exemple des conseils générés

Nom de l'entreprise: Origine Sounds Records

Question 1: Combien d'ordinateurs et de périphériques connectés utilisez-vous dans votre entreprise ?

Réponse: 0-10

Conseil: Vous pouvez sécuriser vos 10 dispositifs en suivant ces conseils :

1. Mettez à jour régulièrement vos logiciels pour combler les failles de sécurité potentielles.
2. Utilisez des mots de passe forts et différents pour chaque appareil pour renforcer la sécurité.
3. Installez et maintenez un logiciel antivirus sur chaque appareil pour détecter et bloquer les menaces.

Question 2: Vos données sont-elles stockées localement sur des serveurs ou dans le cloud ?

Réponse: cloud

- Conseil: 1. Assurez-vous d'utiliser des identifiants forts et de mettre en place l'authentification à deux facteurs.
2. Chiffrez vos données sensibles avant de les stocker sur le cloud pour une meilleure protection.
 3. Gardez vos logiciels et systèmes à jour pour éviter les failles de sécurité potentielles.

Question 3: Comment les données sont-elles partagées au sein de votre entreprise?

Réponse: externe

Conseil: Pour sécuriser le partage de données via un réseau externe, voici deux conseils:

1. Utilisez un protocole de chiffrement fort tel que SSL/TLS pour crypter les données transitant sur le réseau.
2. Mettez en place des mesures d'authentification à double facteur pour renforcer l'accès aux données partagées.

Question 4: Quels types de logiciels utilisez-vous pour la gestion de votre entreprise?

Réponse: ['cms', 'comptabilité', 'Trello']

Conseil:

Pour le logiciel CMS :

1. Assurez-vous de toujours installer les mises à jour de sécurité.
2. Limitez les accès administratifs.

Pour le logiciel de comptabilité :

1. Envisagez d'utiliser une authentification à deux facteurs.
2. Effectuez des sauvegardes régulières.

Pour Trello :

1. Limitez les membres autorisés à accéder aux tableaux sensibles.
2. Utilisez des paramètres de confidentialité adéquats pour chaque tableau

Question 5: Offrez-vous des formations et/ou des séances de sensibilisations à la cybersécurité à vos employés ? Si oui, à quelle fréquence ?

Réponse: non

Conseil: Il est crucial de former vos employés en cybersécurité pour protéger vos données sensibles.

Conseil : Priorisez la formation en cybersécurité dès que possible.

Question 6: Quels sont les réseaux sociaux que vous utilisez dans un cadre professionnel ?

Réponse: ['facebook', 'twitter', 'instagram', '']

Conseil: Sur chacun de ces réseaux sociaux, vous pourriez être confronté à différents risques liés à la cybersécurité.

Voici quelques exemples :

1. Facebook : Sur Facebook, vous pourriez être victime d'attaques de phishing où des cybercriminels tentent de vous tromper en utilisant de faux messages ou liens pour voler vos identifiants de connexion. Vous pourriez également être exposé à des arnaques ou à des faux concours visant à collecter vos données personnelles.
2. Twitter : Sur Twitter, il y a un risque de propagation de fausses informations et de manipulation de l'opinion publique. Vous pourriez également être confronté à des comptes ou à des publications malveillantes visant à vous induire en erreur ou à vous inciter à partager des informations sensibles.
3. Instagram : Sur Instagram, le risque principal est lié à la vie privée et à la sécurité des données. En partageant des photos ou des vidéos, vous pourriez involontairement divulguer des informations personnelles ou sensibles. De plus, des comptes frauduleux pourraient tenter de vous suivre ou de vous contacter pour des desseins malveillants. Il est important de rester vigilant sur ces plateformes et de prendre des mesures pour protéger vos comptes et vos données. En outre, je tiens à vous sensibiliser sur le social engineering, une technique utilisée par les cybercriminels pour manipuler les individus et leur faire divulguer des informations confidentielles. Par exemple, sur Twitter, un attaquant peut se faire passer pour une personne de confiance (comme un membre de votre famille ou un collègue) pour vous inciter à partager des informations personnelles ou à cliquer sur des liens malveillants. Soyez donc prudent et ne divulguez jamais d'informations sensibles à des inconnus, même s'ils semblent être légitimes.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['sauvegarde', 'aucun']

Conseil: Je vous recommande d'utiliser en priorité un antivirus, un pare-feu et un gestionnaire de mots de passe. Ces outils sont essentiels pour protéger vos données et votre système contre les attaques de logiciels malveillants, les intrusions non autorisées et les violations de données. Un antivirus aide à détecter et à supprimer les menaces pour la sécurité, un pare-feu permet de contrôler le trafic réseau et de bloquer les accès non autorisés, tandis qu'un gestionnaire de mots de passe assure la sécurité de vos identifiants en les stockant de manière sécurisée.

Question 8: Comment votre réseau wifi est-il accessible ?

Réponse: un mot de passe moyen (Entreprise12)

Conseil: Non, un mot de passe moyen comme "Entreprise12" n'est pas suffisamment sécurisé. Je vous recommande d'utiliser une passphrase, une phrase composée de plusieurs mots aléatoires pour renforcer la sécurité. Par exemple, "SoleilChatMaison72".

Risques d'un réseau wifi mal sécurisé : accès non autorisé, interceptions de données, attaques de type "homme du milieu".

Question 9: Quelles sont les actions que vous avez entreprises après une cyberattaque ? (Dans le cas où vous n'avez pas subi de cyber attaque, veuillez répondre comme si cela l'était)

Réponse: ['vérification des logs', ' isoler les sauvegarde', ' conservation des preuves via screenshot']

Conseil: Pour être plus efficace lors d'une cyberattaque, vous pourriez également envisager de notifier les autorités compétentes, de mettre en place une communication interne claire à ce sujet, de contacter un expert en cybersécurité pour vous aider dans la remédiation, et de planifier une communication externe si nécessaire. Un plan d'urgence en cas de cyberattaque est crucial pour réagir rapidement et efficacement face à une situation critique, limiter les dommages potentiels, sécuriser les données sensibles, préserver la réputation de l'entreprise et assurer une reprise d'activité plus rapide.

Question 10: Quel est votre domaine d'activité ?

Réponse: Studio d'enregistrement de musique

Conseil: Voici trois exemples d'attaques qui ont visé des entreprises similaires à la vôtre:

1. Phishing : Des employés ont reçu des e-mails frauduleux prétendant être de partenaires pour obtenir des informations sensibles.
2. Ransomware : Un logiciel malveillant a chiffré tous les fichiers de l'entreprise, exigeant une rançon en échange de la clé de déchiffrement.
3. Ingénierie sociale : Des personnes se faisant passer pour des techniciens ont réussi à infiltrer le studio et voler du matériel important.

Résumé global des conseils

Voici un résumé des conseils de cybersécurité pour Origine Sounds Records :

- Pour sécuriser jusqu'à 10 dispositifs :
- Mettre à jour régulièrement les logiciels.
- Utiliser des mots de passe forts et différents pour chaque appareil.
- Installer et maintenir un logiciel antivirus sur chaque appareil.
- Stockage de données dans le cloud :
- Utiliser des identifiants forts et l'authentification à deux facteurs.
- Chiffrer les données sensibles avant de les stocker.
- Garder les logiciels et systèmes à jour.
- Partage de données externes :
- Utiliser un chiffrement fort comme SSL/TLS.
- Mettre en place l'authentification à double facteur.
- Gestion des logiciels d'entreprise :
- CMS : Installer les mises à jour de sécurité et limiter les accès administratifs.

- Comptabilité : Envisager l'authentification à deux facteurs et effectuer des sauvegardes régulières.
- Trello : Limiter les membres autorisés, utiliser des paramètres de confidentialité adéquats.
- Formation en cybersécurité pour les employés.
- Utilisation des réseaux sociaux professionnels :
 - Facebook : Risque de phishing et d'arnaques.
 - Twitter : Risque de propagation de fausses informations.
 - Instagram : Risques liés à la vie privée et à la sécurité des données.
- Outils de sécurité recommandés : antivirus, pare-feu, gestionnaire de mots de passe.
- Sécurisation du réseau wifi avec une passphrase forte.
- Actions à entreprendre après une cyberattaque : vérification des logs, isolation des sauvegardes, conservation des preuves, notification des autorités, communication interne, contact d'un expert en cybersécurité, plan de communication externe.
- Conseils spécifiques pour un studio d'enregistrement de musique concernant les attaques potentielles (phishing, ransomware, ingénierie sociale).