Chapitre

10 La gestion des risques informatiques en PME

- **COMPÉTENCE** Gérer des risques identifiés dans la PME
- **ACTIVITÉ** **2.5.** Participation à la gestion des risques non financiers de la PME
- **TÂCHE** **2.5.4.** Gestion des risques informatiques et des risques liés aux données

Situation professionnelle

L'activité de Régice, entreprise spécialisée dans la construction de piscines et située à Toulon, repose sur un système informatique devant toujours être opérationnel et pour lequel les temps d'accès aux applications et aux données doivent rester satisfaisants. Le système informatique est utilisé par l'ensemble des salariés : les personnels administratifs, dans la réalisation de leurs tâches quotidiennes, mais également les techniciens piscine, lors de leurs déplacements chez les clients. Les techniciens exploitent à distance les ressources informatiques permettant de réaliser les devis ou de passer les commandes nécessaires aux projets des clients.

Estelle Régice, PDG de l'entreprise, s'inquiète car l'actualité évoque régulièrement des situations critiques rencontrées par d'autres entreprises suite à des défaillances liées à leur système informatique. Elle souhaite donc s'assurer que les meilleures dispositions sont prises et procéder aux améliorations nécessaires afin de garantir un fonctionnement optimal de son système informatique.

Comme beaucoup de PME, Régice ne dispose toutefois pas d'informaticien parmi ses effectifs. La dirigeante confie donc cette mission à Thierry Pallu, directeur administratif et financier (DAF), ainsi qu'au prestataire déjà en charge de la maintenance informatique.

Comprendre le contexte

Nathan live ! **Découvrez l'entreprise Régice en vidéo**

1. **Citez quelques exemples de risques qui pourraient concerner le système informatique de Régice.**
2. **Quelles pourraient en être les conséquences ?**
3. **L'absence d'informaticien au sein de l'entreprise est-elle susceptible d'accroître les risques identifiés ?**

VOTRE MISSION

Stagiaire dans l'entreprise, vous êtes associé(e) aux travaux d'amélioration de la sécurité dirigés par Thierry Pallu. Cela nécessite, dans un premier temps, de prendre connaissance de l'existant et de vous familiariser avec le système informatique en place.

TRAVAIL À FAIRE

I. Situer le système informatique dans le système d'information

Vous cherchez d'abord à différencier les différents systèmes de l'entreprise.

1. Quelle distinction faites-vous entre le système d'information et le système informatique de Régice ?

Fiche ressource 1
Annexe 1

2. Donnez quelques exemples de fonctions assurées par le système d'information de l'entreprise.

II. Comprendre la composition d'un réseau informatique

Vous devez maintenant avoir une vue d'ensemble de l'intérêt et du fonctionnement du réseau informatique de l'entreprise Régice. Une documentation actualisée du système informatique, traditionnellement destinée aux personnes susceptibles d'intervenir sur celui-ci (de nouveaux prestataires, par exemple), le permettrait mais celle-ci fait défaut dans l'entreprise.

3. Rédigez cette documentation en présentant une note récapitulant les différentes ressources proposées sur le réseau. Vous serez vigilant(e) à distinguer les éléments matériels et les éléments logiciels.

Fiche ressource 2
Annexe 2

La journée type d'une partie des salariés débute par l'ouverture de leur session sur le serveur, la consultation des messages électroniques reçus et de l'agenda partagé puis l'ouverture du module du PGI nécessaire pour la réalisation des différentes tâches.

Vous devez participer au développement d'une véritable « culture numérique » dans l'entreprise. À ce titre, Mme Régice considère qu'il faut développer la maîtrise et la connaissance qu'ont les salariés au regard des outils utilisés.

COM **4.** Proposez un document, sous la forme qui vous paraît la plus appropriée (texte, schémas, document composite), expliquant aux utilisateurs comment les éléments informatiques du réseau sont sollicités lors des différentes étapes d'une journée type. Vous pourrez par exemple aborder les matériels, les supports de transmission sollicités et mis en œuvre, sans que cette liste soit exhaustive.

Fiche ressource 3
Annexe 2

III. Participer à la prise en charge des risques

Vous poursuivez votre échange avec M. Pallu, qui vous remet également le contrat de maintenance souscrit avec le prestataire.

5. Analysez les risques qui se sont déjà concrétisés, notamment en mentionnant les enjeux de sécurité impactés.

Fiche ressource 4
Annexe 3

6. Repérez les risques existants dans le contrat de maintenance actuel. Préparez le courrier électronique destiné à M. Pallu, en mentionnant également vos préconisations.

Fiche ressource 5
Annexe 4

IV. Appréhender les axes majeurs de la sécurité informatique

Aline Coli, magasinière gestionnaire des stocks, constate un fonctionnement anormal de son ordinateur depuis qu'elle a ouvert une pièce jointe reçue par message électronique. Après un contact avec la hotline du prestataire en charge de la maintenance, un technicien s'est immédiatement déplacé et a constaté que l'entreprise a fait l'objet d'une attaque informatique.

7. Analysez le risque qui s'est matérialisé en déterminant pourquoi l'accès aux données est impossible et en repérant l'erreur commise par Aline Coli.

Fiche ressource 6
Annexes 5 6

8. Déterminez et expliquez les failles de sécurité exploitées puis évaluez les impacts en repérant les enjeux de sécurité concernés.

Dès l'échange en ligne, le prestataire informatique a immédiatement demandé à Aline Coli de débrancher le câble réseau de son poste de travail, avant toute autre manipulation.

9. Pourquoi cette recommandation est-elle importante ?

En définitive, seul le poste d'Aline Coli a été touché, mais cette alerte a été suffisamment grave pour confier un audit de sécurité au prestataire. Vous êtes chargé(e) d'étudier les conclusions de celui-ci en vue d'une communication aux autres salariés.

10. Les données d'Aline Coli sont-elles définitivement perdues ?

Fiche ressource 7
Annexes 7 8

11. Le prestataire propose une sauvegarde en ligne complémentaire à la sauvegarde existante. Est-ce vraiment utile ? Pourquoi ?

12. Faites des recherches et réalisez un comparatif de quelques solutions proposées sur le marché en matière de sauvegarde en ligne. Votre document devra mentionner plusieurs critères de comparaison pertinents.

13. Expliquez en quoi le VPN joue un rôle en matière de confidentialité.

COM **14.** Synthétisez l'ensemble des informations utiles afin de sensibiliser les salariés à la sécurité informatique. Quel document pouvez-vous proposer ? Présentez une ébauche de ce document.

À ce jour, aucune charte d'utilisation des ressources informatiques n'est proposée dans l'entreprise Régice.

15. Après avoir effectué des recherches complémentaires sur Internet, préparez une ébauche de charte informatique en indiquant les principaux points que celle-ci mentionnera.

Fiche ressource 8

Mme Régice et M. Pallu ont assisté à une démonstration en ligne d'un PGI proposé en *cloud computing*. Séduits par la présentation effectuée, ils souhaiteraient approfondir leur réflexion sur cette solution qui modifierait l'organisation actuelle.

COM **16.** Consultez les détails de cette solution et présentez une note de synthèse. Prenez en considération les avantages et les inconvénients associés, ainsi que sa conformité à la réglementation en vigueur.

Fiches ressources 9 10
Annexe 9

DONNÉES DE LA SITUATION

Annexe 1 Entretien avec Thierry Pallu

Vous : Pouvez-vous me donner quelques indications sur votre système informatique ?

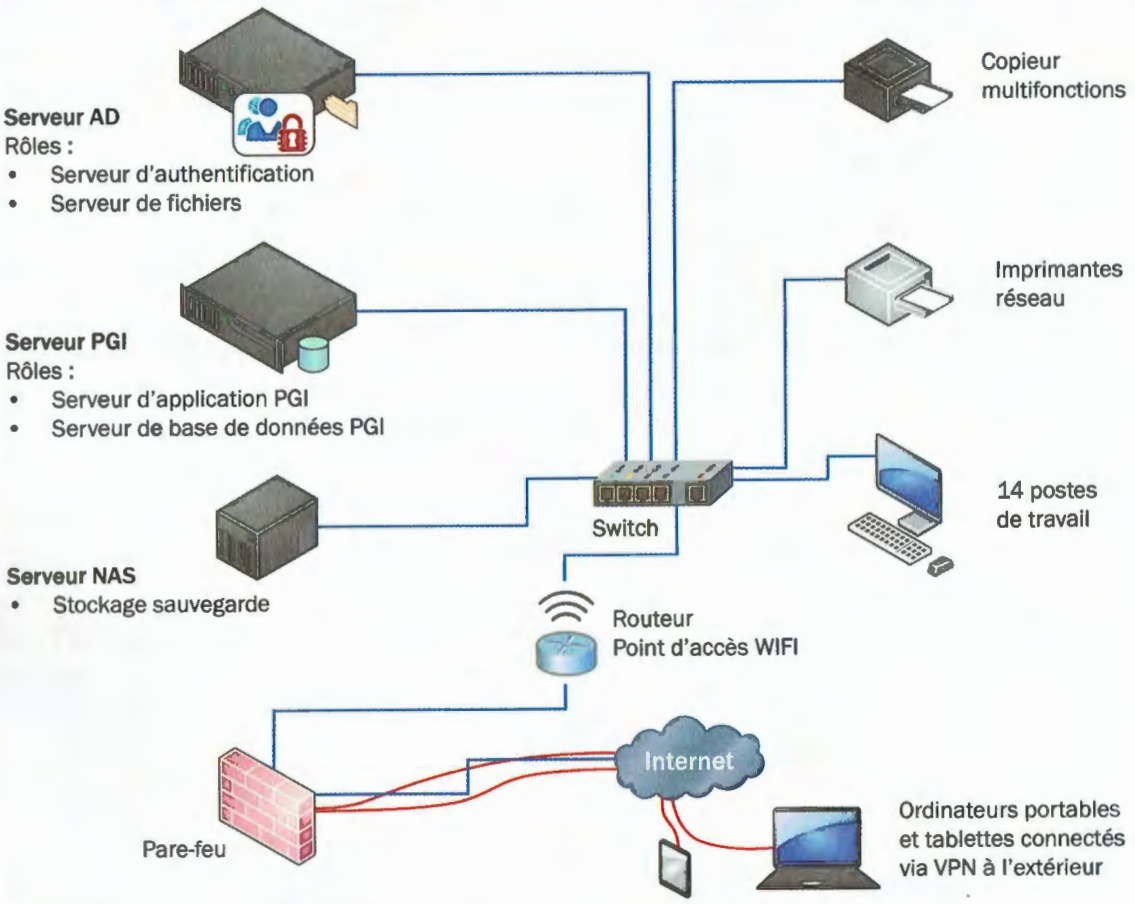
Thierry Pallu : Bien sûr ! Au moins dans les grandes lignes en tout cas. Je ne suis pas informaticien et notre structure est trop petite pour en embaucher un, donc je m'occupe de certains aspects en collaboration avec notre prestataire.

Nous avons une quinzaine d'ordinateurs reliés en réseau et deux serveurs qui centralisent plusieurs ressources. Nous avons également des ordinateurs portables qui sont utilisés par les techniciens lorsqu'ils se déplacent chez les clients. Ils peuvent se connecter à distance à notre système, ce qui permet de gagner beaucoup de temps car ils disposent d'informations en temps réel, telles que le planning des chantiers et les stocks. Ils peuvent, par exemple, réaliser les devis pour les projets de piscines ou prendre des commandes de produits directement chez nos clients.

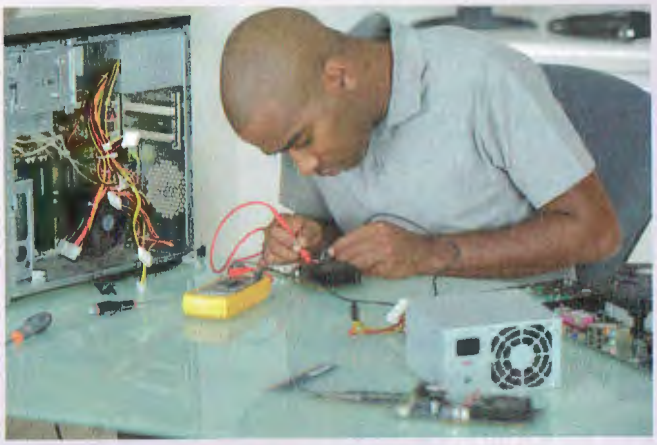
Vous : Et cela fait gagner vraiment beaucoup de temps ?

T. P. : Oui, car une fois ces informations dans notre PGI, cela permet d'affecter immédiatement les équipes et les moyens nécessaires, et de communiquer très rapidement au client les dates prévisionnelles de réalisation de sa piscine ou d'émettre les factures des prestations réalisées, par exemple.

Annexe 2 Schéma du système informatique existant



Annexe 3 Suite de l'entretien avec Thierry Pallu



Vous : Vous m'avez parlé d'un prestataire. Comment sont réparties les tâches entre vous et lui ?

Thierry Pallu : Il prend en charge toute la partie installation, maintenance et dépannage de nos matériels. Il intervient également sur les opérations complexes ou techniques pour lesquelles nous ne sommes pas en mesure d'intervenir. En ce qui me concerne, je gère les comptes des utilisateurs en créant les comptes ou en modifiant les habilitations. J'interviens également sur les paramétrages des applications métiers. Par exemple, c'est moi qui modifie certains éléments du PGI. Mais je ne touche pas à l'installation technique !

Vous : Le prestataire vient-il régulièrement ?

T. P. : Non, la plupart du temps, il intervient lorsque nous le sollicitons. Nous appelons la hotline lorsque nous avons un problème et, en fonction de celui-ci, nous sommes immédiatement dépannés par téléphone. Parfois, le prestataire prend le contrôle à distance du poste de travail lorsque l'intervention est plus complexe. Les seuls cas nécessitant un déplacement correspondent à des pannes matérielles, ou alors lorsqu'il s'agit d'installer un nouvel équipement.

Vous : Cela arrive souvent ?

T. P. : Non, mais pour autant, nous avons déjà fait face à une panne du disque dur sur l'un de nos anciens serveurs. Il a fallu en acheter un nouveau en urgence, réinstaller les logiciels et les paramétrer puis restaurer les données. Nous avons été privés d'informatique pendant trois jours !

Annexe 4 Extraits du contrat de maintenance souscrit

ARTICLE 1 – OBJET

Le Client commandite le Prestataire pour réaliser la maintenance de son parc informatique ci-après dénommé Contrat de maintenance informatique.

Les détails du présent Contrat de maintenance informatique sont les suivants :

- déplacement sur site pour intervention sur le matériel concerné,
- main-d'œuvre pour remise en état du matériel concerné,
- télémaintenance (prise en main à distance) dans la mesure du possible.

Toute intervention complémentaire fera l'objet d'une facturation séparée.

ARTICLE 2 – PRIX

Pour la prestation de service fournie au titre du présent Contrat de maintenance informatique, le Client versera au Prestataire la somme de deux mille euros (2 000 €) HT mensuellement. Le Prestataire établira une facture mensuelle remise au Client par voie postale ou e-mail. [...]

Toute prestation (ou intervention) non prévue au présent Contrat de maintenance informatique donnera lieu à une facturation en sus, sur la base d'un devis accepté.

ARTICLE 3 – EXCLUSIONS

3.1 La responsabilité du Prestataire se limite à l'obligation de remise en état des matériels en panne (couvert par le présent Contrat de maintenance informatique). Elle inclut l'installation du système d'exploitation, l'installation des programmes applicatifs (gestion commerciale, comptabilité...), l'intégration des données (sauvegarde à la charge du client).

▶▶▶

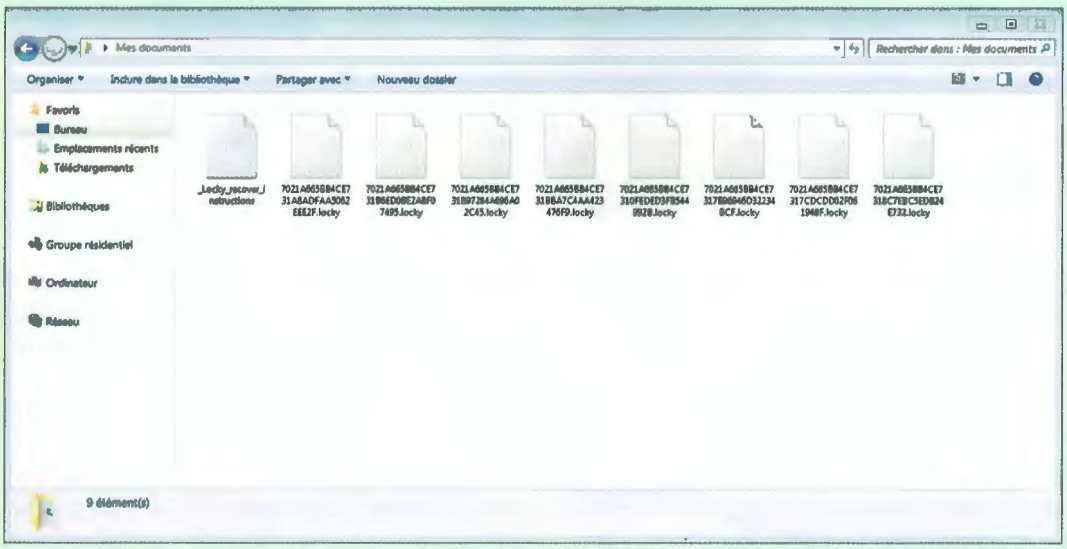
3.2 Sont exclues du présent Contrat de maintenance informatique et donneront lieu à une facturation séparée les interventions dues aux faits suivants :
• non-respect des normes d'entretien par le Client,
• matériel remplacé,
• modification des spécifications des machines sans prévenir le Prestataire,
• variation ou coupure électrique,
• virus, logiciels malveillants ou intrusions,
• réparation ou entretien réalisé par des personnes étrangères au Prestataire,
• remplacement des pièces défectueuses sans accord du Prestataire,
• remplacement des consommables (toners, cartouches, tambour...).

[...]

ARTICLE 5 – DÉLAI
Les interventions ont lieu au plus tard dans les délais suivants :
• intervention H+4 en télémaintenance,
• intervention H+8 sur site,
• pas de limite sur le nombre d'interventions.
Les interventions s'effectuent du lundi au vendredi inclus, aux horaires du prestataire (9 h-12 h et 14 h-18 h). Les jours fériés sont exclus.

Annexe 5 Fichiers d'Aline Coli, magasinière

Aline Coli ne retrouve plus les fichiers qu'elle a enregistrés sur son poste de travail. Au lieu des fichiers de traitement de texte, tableur et autres, il n'y a plus que des fichiers comportant l'extension « .locky » :



Annexe 6 Bulletin d'alerte du CERT* (extraits) présenté par le prestataire

Objet : campagne de messages électroniques non sollicités de type Locky

1 – Risque(s)

Installation d'un logiciel malveillant de type Locky.

2 – Systèmes affectés

Tous les systèmes d'exploitation Windows peuvent être victimes de ce logiciel malveillant.

3 – Résumé

Depuis la mi-février 2016, le CERT-FR constate à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles anti-pourriel est relativement faible. Ces pourriels ont pour objectif la diffusion du rançongiciel Locky.

Un rançongiciel est un programme malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles depuis le compte utilisateur dont la session est compromise. Celui-ci est exécuté, dans le cas présent, par une action de l'utilisateur. La victime est ensuite invitée à verser de l'argent afin que l'attaquant déchiffre les fichiers ciblés.

Dans le cadre de cette campagne, et d'après les échantillons que le CERT-FR a observés, la diffusion de Locky s'effectue par l'intermédiaire d'un pourriel dans lequel se trouve une pièce jointe au format « .doc ». Ce document Microsoft Office contient un texte illisible ainsi qu'un message indiquant la nécessité d'activer les macros pour l'affichage correct du message. Macro dont l'objectif est la récupération puis l'exécution du malware. L'exécution de ce dernier entraîne le chiffrement des données et les fichiers sont renommés avec l'extension « .locky ».

[...]

4 – Solution

Mesures préventives

Le CERT-FR recommande de sensibiliser les utilisateurs aux risques associés aux messages électroniques pour éviter l'ouverture de pièces jointes [...]. Plus généralement, il convient de mettre à jour les postes utilisateurs [...] dans le cas où le code malveillant (ou une variante) exploiterait une vulnérabilité logicielle.

Enfin, le CERT-FR recommande d'effectuer des sauvegardes saines et régulières des systèmes et des données (postes de travail, serveurs) puis de vérifier qu'elles se sont correctement déroulées. Les sauvegardes antérieures ne doivent pas être écrasées (cas où une version chiffrée aurait été sauvegardée). Les sauvegardes doivent être réalisées en priorité sur les serveurs hébergeant des données critiques pour le fonctionnement de l'entité. Celles-ci doivent être stockées sur des supports de données isolés du réseau en production.

www.cert.ssi.gouv.fr

* CERT : *Computer Emergency Response Team*, centre d'alerte et de réaction aux attaques et incidents informatiques.

Annexe 7 Quelques règles informatiques mises en œuvre

- Chaque utilisateur dispose de ses propres identifiants et mots de passe personnels. Ceux-ci doivent rester strictement confidentiels.
- Les droits (ou habilitations) sont paramétrés en fonction des attributions de chaque salarié. Ils ne doivent en aucun cas être contournés. En cas de nécessité, ils peuvent être modifiés après demande justifiée auprès de l'administrateur.
- Les utilisateurs s'engagent à enregistrer leurs fichiers dans leur emplacement personnel sur le serveur de fichiers ou sur un des emplacements réseau partagé afin de bénéficier d'une sauvegarde automatisée. Tout fichier stocké ailleurs l'est sous la pleine responsabilité du salarié en cas de perte ou compromission.
- Les données des serveurs sont sauvegardées tous les soirs sur le NAS (*Network Attached Storage* : serveur de stockage en réseau).

Annexe 8 Extrait des conclusions de l'audit réalisé par le prestataire

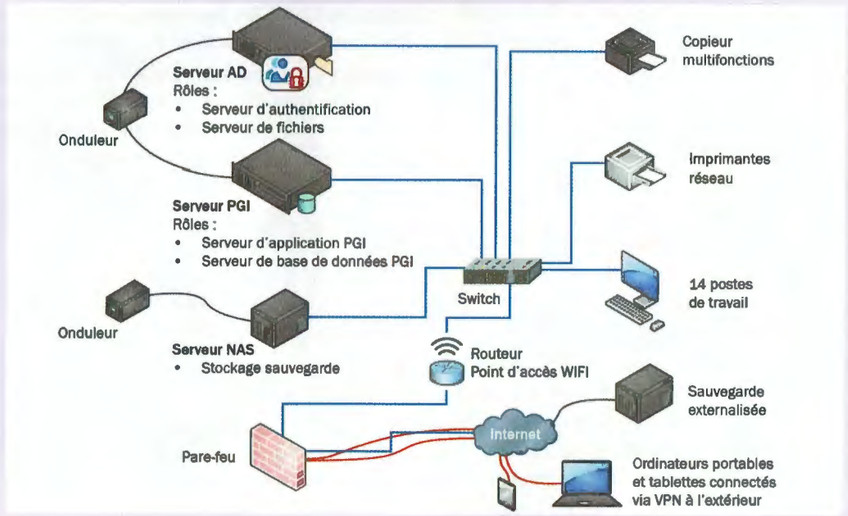
1. Points positifs du système existant

- Les utilisateurs font tous l'objet d'une authentification, la gestion des mots passe et leur renouvellement sont effectués correctement.
- Le réseau est sécurisé grâce au pare-feu qui fait l'objet d'un paramétrage adéquat.
- Les connexions depuis l'extérieur sont convenablement sécurisées grâce au VPN[1].
- Une politique de sauvegarde régulière est en place sur les serveurs et les données sont stockées sur un autre support (NAS[2]).

2. Préconisations et évolutions nécessaires

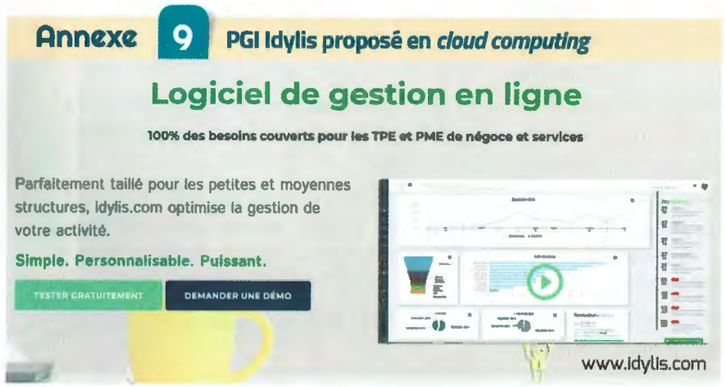
- Suite aux entretiens réalisés, les utilisateurs doivent être davantage informés des risques informatiques auxquels vous êtes exposés. Une sensibilisation doit être envisagée.
- Une gestion centralisée d'une suite de sécurité antivirale et antimalware est nécessaire. Ce rôle peut être ajouté au serveur existant sans difficulté. Il permettra de déployer en temps réel les mises à jour antivirales et d'effectuer une remontée régulière des informations et alertes.
- Il est nécessaire d'améliorer la sauvegarde existante en disposant de sauvegarde hors site. Nous vous incitons à recourir à une solution de sauvegarde en ligne.
- Les serveurs ne sont pas protégés. L'installation d'onduleurs est indispensable.

Schéma du système cible



1. *Virtual Private Network*, réseau privé virtuel.
2. *Network Attached Storage*, boîtier de stockage en réseau.

Annexe 9 PGI Idylis proposé en *cloud computing*



1 Système d'information et système informatique

I La notion de système d'information (SI)

Un SI correspond aux différents moyens mis en œuvre afin de collecter, de mémoriser, d'utiliser et de diffuser de l'information au sein de l'entreprise et avec son environnement. Il comprend :
– des moyens **humains**, qui correspondent aux personnes qui reçoivent, utilisent et émettent de l'information (acteurs) ;
– des moyens **techniques, matériels et immatériels**, c'est-à-dire des outils exploités dans la manipulation des informations, souvent le système informatique (matériels tels qu'ordinateurs et logiciels mis en œuvre) ;
– une **dimension organisationnelle** avec des **procédures** et des **méthodes** correspondant aux règles suivies et appliquées dans la réalisation des activités afin d'atteindre les résultats souhaités.
Le SI permet donc le stockage et le traitement d'informations ayant une origine interne ou externe (en provenance de l'environnement de l'entreprise et de ses partenaires) et les restitue sous une forme utilisable au moment opportun pour faciliter la prise de décision et le fonctionnement de l'entreprise.
Le **système informatique** n'est donc qu'une partie du SI, de nature **technologique**, et ne doit pas être confondu avec lui.

II Les fonctions du système d'information

Un SI remplit quatre fonctions essentielles.

Fonction	Explication
L'acquisition	Il s'agit d'obtenir des informations, qu'elles proviennent de **sources externes** (partenaires extérieurs tels que les fournisseurs, les institutions financières, les administrations…) ou **internes** (services de l'organisation qui produisent de l'information stockée dans des fichiers ou des documents internes). C'est à ce stade qu'en matière de sources externes, la **veille informationnelle** et l'utilisation d'outils appropriés sont importantes.
La mémorisation	Il s'agit de stocker les informations de manière durable afin de permettre une utilisation ultérieure. Souvent, l'enregistrement des informations est réalisé sur des supports informatisés et organisés en bases de données.
L'exploitation	Cela correspond à l'utilisation des informations par des programmes informatiques ou des interventions manuelles afin de prendre des décisions ou de produire de nouvelles informations.
La diffusion	Il s'agit de transmettre les informations aux acteurs, internes ou externes.

III Le système informatique

Le système informatique est composé d'**éléments matériels** pouvant prendre différentes formes : ordinateurs fixes ou portables, périphériques (imprimantes, scanners, copieurs multifonctions…), équipements de communication en réseau. Il comprend également des **éléments immatériels**, principalement les différents logiciels utilisés dans l'entreprise.