Annexe: messagerie/calandrier

1.1 Généralités

Ce chapitre est consacré aux fonctionnalités destinées à la communication par e-mail et à la planification au moyen du calendrier. Des packs de solutions offrant des fonctionnalités supplémentaires permettant la collaboration sont également disponibles. Naturellement, il est possible de considérer également ces packs de solutions. Cependant, nous faisons consciemment la différence entre ces fonctionnalités, car des systèmes supplémentaires entreraient en ligne de compte dans le choix de variantes à implémenter.

Par principe, un message e-mail n'est pas protégé : ni contre sa lecture par des tiers, ni contre sa manipulation. Il est donc important d'implémenter des mesures de sécurisation locales, mais elles seront moyennement utiles sans la prise en compte de l'envoi effectif des messages.

1.2 Besoins

- ☐ Est-il nécessaire de permettre le traitement des données de la messagerie / du calendrier via plusieurs plateformes/systèmes d'exploitation différents ?
- ☐ Faut-il que les données de la messagerie / du calendrier soient traitées sur plusieurs terminaux différents (par ex. ordinateur/portable, tablette, téléphone portable) ?
- ☐ Souhaitez-vous exploiter une solution largement répandue, par exemple pour que votre nouveau personnel s'y retrouve plus facilement dans un environnement informatique familier ?
- ☐ Souhaitez-vous avoir recours à des filtres anti-spam performants et mis à jour en permanence ?
- ☐ Souhaitez-vous disposer de fonctionnalités anti-virus et anti-hameçonnage performants et mises à jour en permanence ?
- ☐ Favorisez-vous un cryptage simple (et donc moins bien sécurisé) des messages e-mail ?
- ☐ Préférez-vous un cryptage hautement sécurisé des messages e-mail ?
- ☐ Voulez-vous que les données du calendrier soient partagées et/ou mutuellement affichables en interne en toute simplicité et efficacité ?
- ☐ Voulez-vous que les données du calendrier soient rendues accessibles à des tiers en toute simplicité ?
- ☐ Souhaitez-vous que l'accès aux données soit protégé par l'authentification multi-facteurs ?
- ☐ Avez-vous des exigences système qui ne permettent qu'une seule solution : soit « on-premise », soit SaaS ?

1.3 Recommandations

Si vous

- ☐ disposez de peu de ressources internes compétentes en informatique
- ☐ exploitez déjà (une partie) des solutions dans le cloud / sous forme de SaaS
- ☐ souhaitez des mises à jour à intervalles réguliers
- ☐ ne voulez pas devoir vous préoccuper de travaux de maintenance, etc.
- ☐ accordez de l'importance aux technologies les plus récentes en matière d'anti-spam et d'anti-hameçonnage
- ☐ voulez disposer de nouvelles fonctionnalités rapidement/immédiatement
- ☐ avez besoin d'un système garantissant une disponibilité élevée (par ex. données redondantes)
- ☐ voulez continuer de pouvoir effectuer une intégration éventuelle dans d'autres systèmes comme auparavant
- ☐ voulez crypter et/ou signer les messages e-mail
- ☐ voulez crypter et signer l'ensemble de vos communications par e-mail
- ☐ considérez comme important le lieu de stockage des messages e-mail et des données qu'ils contiennent
- ☐ (à noter : envoi et réception externes)
- ☐ disposez déjà de fonctionnalités de sécurité (par ex. anti-spam et anti-hameçonnage) ; celles-ci sont possibles aussi bien dans les solutions « on-premise » qu'intégrées aux options SaaS

Nous vous recommandons d'opter pour un système de messagerie/calendrier basé sur SaaS.	**Il est possible d'envisager une installation locale / « on-premise ». En plus du cryptage des courriels, vous aurez aussi la possibilité d'agir au niveau local en toute indépendance.**

1.4 Exemple pratique: SaaS

Une société fiduciaire occupant environ 15 collaboratrices et collaborateurs adopte en règle générale des installations « on-premise ». Tous ses logiciels sont installés sur sa propre infrastructure informatique locale : archivage des données, programmes financiers, programme fiscal, messagerie/calendrier, système de gestion qualité, etc. Il existe la possibilité de traiter les messages e-mail en externe. Par ailleurs, suite à l'obligation de travailler à domicile, une option d'accès limitée mais sécurisée a été mise en place pour permettre d'accéder aux programmes financiers hors site. La philosophie de l'entreprise préconise en principe le travail au bureau, car il présente l'avantage non seulement de la disponibilité de toutes les données (électroniques et physiques) sur place, mais aussi des échanges entre collaborateurs/trices.

La nécessité de remplacer l'ensemble du hardware (garantie arrivée à échéance) a été l'occasion pour la société d'évaluer plusieurs scénarios : de l'installation complète sur site avec un accès externe réduit à un outsourcing total de l'infrastructure.

Décision du client : déployer la messagerie et le calendrier en tant que première solution SaaS. Parmi les arguments principaux ont figuré la sécurité améliorée et l'élimination des travaux de maintenance. Les solutions restantes demeureront installées sur site, ce qui est notamment attribuable à la non-disponibilité de certains systèmes en tant que solutions SaaS. Il s'agit pour l'agence de faire ses premiers pas pour se familiariser avec les solutions SaaS.

.

1.5 Exemple pratique: «on-premise»

Une société fiduciaire exploite un hardware moderne dont la garantie du fabricant sera encore longtemps valable. Saisissant l'occasion d'une mise à jour logicielle, on a pourtant évalué l'utilité d'une solution SaaS. Malgré la sécurité plus élevée offerte par la solution SaaS, le client a décidé de rester « on-premise » pour l'installation de sa messagerie / son calendrier. Il a considéré comme prioritaire de continuer à utiliser l'infrastructure matérielle existante et de bénéficier de mises à jour peu onéreuses. Une solution SaaS sera implémentée dès que les garanties du hardware arriveront à échéance.