

Infrastructure

Liste des éléments à prendre en considération pour réaliser une infrastructure client de qualité.

Les éléments à penser

Une bonne infrastructure doit contenir les éléments suivants (à minima) :

- Emails
- Stockage des données
- Protection contre les menaces
- Reprise d'activité
- Suite de bureautique
- Applications métier
- Connexion Internet
- WIFI
- Téléphonie
- [facultatif] Protection des données
- [facultatif] Gestion centralisé du parc

Emails

Le bon conseil est de mettre les emails sur Office 365 en général. Les deux seuls cas où une autre solution est conseillé est :

- Si les emails sont sensibles et ne peuvent pas être stocké dans n'importe quel pays.
- Si la société a plus de 100 utilisateurs, la licence Exchange est potentiellement moins chère.

Attention, nous recommandons de migrer au plus vite les sociétés utilisant des boites POP ou IMAP. Ces systèmes ne garantissent pas la bonne sauvegarde des données.

Stockage des données

Il y a deux principales familles de stockage pour les données :

- Stockage Cloud
 - Dropbox
 - OneDrive / SharePoint Online
- Stockage sur serveur
 - SMB
 - SharePoint
- Stockage sur NAS

Stockage Cloud

Le stockage Cloud peut être lent, principalement s'il y a un nombre important d'utilisateurs sur la même connexion. On peut retrouver une bonne partie des fonctionnalités possibles sur un serveur avec un stockage Cloud OneDrive. Par contre OneDrive est limité à 1To sur les licences Office365 destinées aux petites entreprises (<100 utilisateurs).

Le stockage Dropbox est aussi possible. Il n'a aucune limite de taille sur la version professionnelle mais est plus couteuse et permet moins d'options que OneDrive. Cette seconde solution est à utiliser dans le cas où les utilisateurs sont déjà habitués à l'utiliser.

Stockage sur serveur

Le partage de fichier sur Windows Server permet d'avoir une gestion des droits plus fin. Par contre il y a quelques inconvénients à son usage. Il y a un "versionnement" des données mais à heure fixe. Deux modifications effectués à intervalle trop court ne seront pas récupérable.

Il y a toutefois la solution SharePoint qui permet d'avoir les mêmes fonctionnalités qu'un cloud OneDrive / SharePoint Online, mais nécessite des licences à payer.

Dans le cadre entreprise, Microsoft recommande d'utiliser SharePoint pour les documents (fichiers < 100MB) et utiliser le partage de fichier pour les fichiers multimédia (>100MB) comme les images CD, vidéos, etc...

Stockage sur NAS

Le stockage sur NAS est une solution "local" pas chère mais peu recommandé. Il n'y a pas de versionning sur ce type de stockage et la sauvegarde est souvent une bidouille impossible à monitorer.

Attention, les NAS ne sont souvent pas à usage professionnel et il n'y a pas d'assurance sur le service client. Il peut falloir un mois entier avant de pouvoir restaurer les données. Il vaut donc mieux proposer à minima deux NAS.

Protection contre les menaces

La protection des menaces passe par trois éléments :

- Protection réseau (pare-feu)
- Protection des logiciels (anti-virus)
- Protection contre le spam / phishing (anti-spam)

Microsoft propose déjà tous ces éléments, mais ne sont souvent pas suffisants. En effet, un virus n'est efficace que s'il contourne les protections par défaut de Microsoft. Tous les virus en circulation ont donc cette aptitude.

réseau (pare-feu)

Nous sommes revendeur Clavister et nos techniciens sont formés sur ce produit. Nous recommandons exclusivement Clavister pour les clients qui souhaite cette protection, avec la licence qui va bien.

Sans la licence, nous ne pouvons pas faire de restauration aisée en cas d'erreur de configuration.

Les clients déjà pourvus d'un pare-feu sont aussi encouragés à passer sur Clavister afin d'homogénéiser le parc et pour que nos techniciens interviennent plus facilement.

logiciels (anti-virus)

Nous sommes revendeur de deux solutions anti-virus :

- BitDefender
- Symantec Norton

Les deux solutions sont valables. Toutefois nos techniciens sont plus aptes à utiliser BitDefender (qui a aussi la possibilité de faire anti-spam pour Exchange). Les études de performances montrent aussi que BitDefender est plus puissant que Norton.

spam / phishing (anti-spam)

Attention, Exchange ne possède pas d'anti-spam par défaut !

Office 365 possède un anti-spam basique et souvent suffisant. Toutefois l'anti-spam d'Office365 est limité et peu configurable. Beaucoup de spam et hameçonnage passent malgré la protection. Il peut être intéressant de proposer MessageLabs en prime.

MessageLabs est très complet et correctement configuré parvient à bloquer toutes les menaces. Il peut être employé avec Exchange ou Office365. De plus nos techniciens sont formés à ce produit dont nous sommes aussi revendeur. C'est une des meilleures solutions à proposer aux clients.

BitDefender a aussi une solution anti-spam efficace mais n'est disponible que sur Exchange.

Reprise d'activité

Il faut penser à une solution alternative en cas de panne de n'importe quel élément de l'infrastructure. Il faut aussi penser à l'environnement pour se prémunir des pannes :

- Température de la salle (clim ? capteur ?)
- Alimentation des systèmes [NAS/Serveurs] (onduleur ?)

En cas de panne sur un équipement, combien de temps avant le retour en production suivant la panne ? Combien de temps acceptable ? Sous combien de temps le support des différents éléments de l'infrastructure peut intervenir ?

Suivant les réponses aux problématiques de reprise d'activité et de l'infrastructure il faut

probablement doubler les serveurs / stockage / connexions réseaux.

Suite de bureautique

Tous les postes en entreprise doivent être équipés d'une licence. Il y a trois types de licences.

Petite et moyenne entreprise

Convient pour les travailleurs indépendants, mais peu recommandé. Dans un cadre général il vaut mieux utiliser un abonnement Office365 entre 1 et 50 utilisateurs.

Office365

Convient pour la plupart des cas.

Licence volume

La licence en volume est potentiellement plus rentable pour les entreprises de plus de 50 utilisateurs pouvant se permettre de garder une version Office pendant 10 ans (temps maximum de support d'une version Office).

Applications métier

Si une société a des applications métier, il peut y avoir des spécifications particulières à prendre en compte dans le dimensionnement du serveur.

Connexion Internet

Il faut penser aux connexions Internet. Il est préférable d'avoir au moins une connexion "professionnelle" (rétablissement garanti sous 4h), au moins une connexion "bridge" (pour le VPN) et au moins une connexion fibre (si disponible). Une seule connexion peut répondre à plusieurs caractéristiques et il faut au moins deux connexions.

Le VPN ne peut pas être configuré sur toutes les box, d'où la nécessité du Bridge.

Fournisseur	Professionnel	Bridge	Fibre
Orange	Oui	Non	Oui
SFR	Oui	Non	Oui
Bouygues	Oui	Oui	Oui
OVH	Oui	Oui	Non
Free	Non	Oui	Oui

Pour la téléphonie, s'il n'y a pas de fibre, il vaut mieux un abonnement SDSL supplémentaire.

WIFI

Pour le Wifi, il est peut recommandé d'utiliser le WIFI des box. De plus il n'est pas possible d'utiliser le wifi d'une box en "Bridge".

Le mieux est d'utiliser des bornes Wifi dédié.

Attention, une borne Wifi a besoin d'une alimentation. De base, une borne est alimenté par PoE. Si aucun commutateur PoE n'est disponible, alors il faut prévoir une alimentation électrique à commander séparément.

Réseau GUEST

Le réseau GUEST est conseillé pour être communiqué aux visiteurs d'une société. C'est un réseau qui ne donne pas accès aux ressources de l'entreprise et ainsi éviter que des personnes volent des données, s'infiltrant sur les postes ou utilisent illégitimement les imprimantes.

Pour pouvoir mettre en place un réseau GUEST, il faut un pare-feu de préférence matériel (Clavister ?) et un commutateur compatible VLAN. Pour ainsi dire tous les commutateurs manageables sont compatibles VLAN. Dans certains cas très spécifique il est possible de faire autrement.

Téléphonie

La téléphonie est à prendre en compte sur l'infrastructure même si nous ne sommes pas en charge de son déploiement. En effet, s'il s'agit d'une téléphonie analogique, il faut prévoir une prise téléphonique dédié par poste.

Dans le cadre d'une téléphonie IP, il faut se mettre en accord avec le téléphoniste pour savoir s'il passe par un réseau spécial avec un commutateur spécifique. Si c'est le cas, il faut tout de même une prise par téléphone. Si le commutateur est partagé avec le réseau, il n'est pas forcément nécessaire d'avoir une prise dédié au téléphone (suivant le modèle).

Attention, l'usage du téléphone et du PC sur la même prise peut ralentir la connexion du PC si le téléphone n'est pas gigabyte.

Protection des données

Il est possible de protéger les documents et empêcher qu'ils soient sortis du parc informatique. Cette configuration est plus spécifique et nécessite une étude plus poussée.

Gestion centralisé du parc

Les postes du parc peuvent être géré de façon centralisé via un Active Directory. L'usage d'un Active Directory permet aux techniciens d'être plus réactifs sur la configuration des appareils et pouvoir changer les mots de passes des utilisateurs en cas de nécessité.

Il est possible de ne pas avoir de gestion centralisé du parc, mais toute opération sur les comptes utilisateurs (création / suppression / réinitialisation du mot de passe) et déploiement des imprimantes. Ce qui implique des frais supplémentaires sur les installation et désinstallation des collaborateurs.

From:

<https://wiki.sadmin.fr/> - **Technisys**

Permanent link:

<https://wiki.sadmin.fr/systemes/infrastructure>

Last update: **20/03/2018 11:51**

