GMSI16

Nicolas Gérard

Sébastien Lavaux

Quentin Zantedeschi

CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

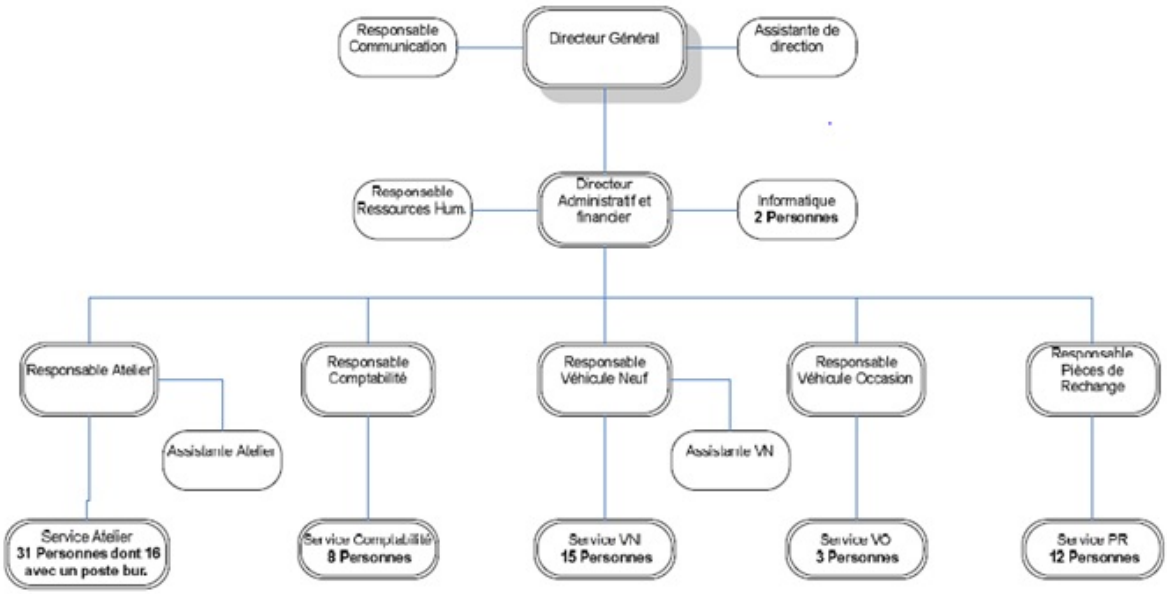
PROJET SAS

Table des matières

MISE EN SITUATION

Notre société, Axolotl IT, est un prestataire informatique de la région Rhône-Alpes. Un concessionnaire automobile, AutoConcept, souhaite externaliser les prestations informatiques qui sont actuellement gérées par deux informaticiens en interne. D'autres entreprises concurrentes sont aussi en course pour obtenir la gestion du parc informatique. Le directeur technique nous charge de réaliser une partie de l'étude de l'avant-vente et nous annonce qu'en cas d'obtention du marché, l'un des deux informaticiens de « AutoConcept » sera recruté. Nous serons donc chargés de son accueil et son accompagnement au sein de l'entreprise Axolotl IT.

La société « AutoConcept » est une franchise mandataire basé sur Vénissieux proposant des prix cassés sur la vente d'automobiles neuves. Le parc informatique est composé de 68 postes répartis dans tous les services de la concession.



PRÉSENTATION DE L'ENTREPRISE

Depuis 2013, Axolotl IT, une jeune start-up Lyonnaise, met en place des solutions innovantes dans le domaine des infrastructures réseaux et de la maintenance informatique, aussi bien pour l'industrie pharmaceutique, que pour le BTP, les concessions automobiles ou bien les grandes surfaces. Axolotl IT gère la plupart des incidents utilisateurs.

Le nom de la société est en référence à l'Axolotl, une espèce d'urodèles de la famille des amphibiens qui a la particularité de pouvoir régénérer ses organes endommagés ou détruits, et qui peut également s'adapter afin de vivre sur terre et non plus dans l'eau. Notre cœur de métier étant notamment la sécurité, la sauvegarde et la restauration de données, tel un Axolotl nous nous adaptons à chaque situation.

Nous faisons également don d'une certaine somme chaque année à l'IFAW « International Fund for Animal Welfare », don qui sert à financer des actions pour la protection des animaux dans le monde entier (l'Axolotl étant en voie d'extinction).

Adresse :

Axolotl IT

9 Rue Léon Blum,

69100 Villeurbanne

Contact : axolotlit@gmail.com

NOTE DE SYNTHÈSE

o Utilisation des outils informatiques en entreprise :

L'outil informatique est depuis quelques années présent dans chaque société, il est devenu un outil nécessaire et même l'outil principal de beaucoup d'utilisateurs, c'est pourquoi son utilisation est réglementée par la CNIL (la Commission Nationale de l'Informatique et des Libertés). La CNIL a été créée afin de garantir une vie privée aux utilisateurs en garantissant leurs libertés, mais en limitant également le contrôle de l'employeur tout en lui donnant la possibilité de fixer lui-même des limites à l'usage pour la sécurité du réseau de l'entreprise ainsi que pour garder la productivité de l'entreprise.

o Contrôle de l'utilisation d'Internet et de la messagerie

L'utilisateur doit prendre connaissance que l'employeur peut contrôler et limiter l'utilisation d'Internet en utilisant des filtres de sites non productifs (Facebook, Twitter, YouTube, Instagram etc…), à caractère pornographique, pédophile, contraire aux bonne mœurs ou portant atteinte à la dignité humaine (photo dégradante etc …) et également éviter les sites de téléchargement illégaux et les échanges de données non autorisés (P2P etc…). Ce filtrage est quant à lui contrôlé par le firewall de l'entreprise. La messagerie des utilisateurs peut aussi être contrôlée via des outils de mesure de la fréquence des envois ou de la taille des messages pour éviter tout blacklisting et une application de filtre « anti-spam » peut être utilisée afin de réduire les chances d'infection de poste utilisateur.

Toutes ces mesures ont pour objectif :

- √ D'éviter des attaques virales et de pouvoir garder en sécurité les réseaux de la société.
- √ De limiter les abus dans l'utilisation à titre personnel de la messagerie ou d'Internet en évitant tous les sites non productifs déjà listés ci-dessus.

Il faut donc bien comprendre que par défaut tout courriel ayant un caractère dit professionnel peut être lu par l'employeur : « Les tribunaux considèrent que tout message reçu ou envoyé depuis le poste de travail mis à disposition par l'employeur a par principe un caractère professionnel. Dans ce cas, l'employeur peut le consulter […] » (cf Annexe : doc CNIL). L'employeur a également la possibilité de prendre connaissance des sites consultés par

son employé même en dehors de sa présence pour vérifier la productivité de son personnel lors des heures de travail.

o Un grand pouvoir implique de grandes responsabilités

Bien entendu, les entreprises ne sont pas là pour appliquer une politique de surveillance enlevant toute vie privée aux utilisateurs, c'est pour cela que des limites sont également appliquées au contrôle de l'employeur.

Il n'est par exemple en aucun cas possible qu'un responsable de service d'AutoConcept puisse recevoir une copie automatique de messages écrits ou reçus par ses employés. En effet, ces derniers ont droit, même au travail, au respect de leur vie privée et au secret de leurs correspondances, même si une interdiction de l'utilisation des outils de l'entreprise à des fins personnelles est stipulée.

- √ Il est conseillé aux utilisateurs de créer un répertoire intitulé « messages privés » ou « personnel » pour mettre une barrière entre ce qui peut être consulté ou non sans autorisation.
- √ Il est également interdit d'utiliser des « keyloggers », des logiciels espions, permettant d'enregistrer à distance la globalité des actions faites sur l'ordinateur par les utilisateurs, sauf si bien sûr, en cas de circonstance exceptionnelle liée à un impératif de sécurité.

Cette méthode de surveillance est illicite et cela peut être puni par le code pénal via l'article 226-1 : « Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui » :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Deux types de solutions sont à retenir pour la sécurité des données, ainsi que pour la supervision du réseau et donc la continuité de service.

Il existe tout d'abord des solutions légales (contrairement aux keyloggers) permettant d'avoir un maximum de données sur l'utilisation qu'ont les employés de l'outil informatique, principalement dans un but de sécurité des données.

On pourra citer notamment Varonis, Stealthbits ou bien Netwrix, qui proposent des solutions complètes, avec des fonctionnalités poussées permettant par exemple de :

- √ détecter la suppression d'un grand nombre de fichiers sur le réseau
- √ détecter de nombreux changements de mots de passe
- √ détecter des tentatives d'accès sur des dossiers "interdits"
- √ détecter des modifications de fichiers à une vitesse "non humaine" qui peuvent être dues à un Cryptolocker

Ces solutions proposent en général des fonctions de recherche très précises, pouvant permettre de voir qui a fait quoi, sur quel fichier, et quand. Elles permettent donc d'agir dans l'urgence, afin de "limiter la casse" ou bien par la suite de restaurer des sauvegardes de données perdues.

Le second point important est donc la supervision du réseau et de l'ensemble des services, dans le but d'une plus grande continuité de service. Il existe des solutions utilisant des "capteurs", afin de détecter les éventuelles pannes de services, de vérifier l'état des connexions grâce à des requêtes "ping", de prévenir de l'utilisation des stockages ou bien de la ram, etc. On pourra citer par exemple Nagios, Shinken, Centreon, PRTG…Ces solutions proposent des fonctionnalités diverses, en fonction de la licence choisie, mais elles se basent globalement sur le même principe de fonctionnement : capteurs/affichage d'alertes. La page de visualisation de l'ensemble des alertes peut ainsi être affichée sur un écran de surveillance dédié, afin d'agir dès la visualisation de l'alerte, pour corriger le problème.

Ces deux types de solutions sont particulièrement efficaces pour sécuriser les données et garder une continuité de service optimale. Cependant, l'une des principales sources pouvant amener à une multitude de problèmes doit également être contrôlée un minimum, il s'agit d'Internet.

o Filtrage de contenus

Il est donc important d'utiliser une solution de filtrage de contenu en entreprise. Ainsi, 80% des entreprises filtrent le contenu d'Internet, selon la société Olfeo. Non seulement cela peut permettre d'éviter que les utilisateurs naviguent sur des sites à caractère illégal, mais cela peut permettre également de sécuriser un peu plus le réseau informatique. En effet, un grand nombre de sites peuvent nuire à la sécurité du réseau, principalement les sites de téléchargement illégaux, qui fournissent parfois des fichiers infectés. Adopter une solution de filtrage peut également permettre d'améliorer la productivité de son entreprise en bloquant des sites tels que les réseaux sociaux ou bien les sites de jeux en ligne. Enfin, certains sites non productifs tels que les sites de streaming ou tout simplement les sites de téléchargements, sont des grands consommateurs de bande-passante. Un filtrage de ces sites permettra donc à l'ensemble des utilisateurs de pouvoir travailler convenablement, sans perte de débit.

Il existe également un autre aspect intéressant souvent associé à l'utilisation d'une solution de filtrage, il s'agit des "logs", ou historique d'événements en français. Ainsi, les FAI (Fournisseur d'Accès à Internet) ont l'obligation de garder les logs de leurs utilisateurs pendant une durée d'un an. Depuis 2006, une entreprise qui fournit un accès à Internet, même gratuit, au public, a également les mêmes devoirs qu'un FAI et doit donc garder un historique des utilisations de l'accès qu'elle fournit. De plus, en cas d'utilisation du réseau de l'entreprise pour effectuer des activités illégales, le salarié est responsable, mais également le dirigeant de l'entreprise, et le responsable informatique. Il s'agit donc de trouver un juste milieu, en respectant à la fois les lois sur les libertés des utilisateurs (ne pas utiliser de keyloggers, ne pas consulter les mails des dossiers personnels…), mais également en limitant la consultation des contenus (bloquer les sites de téléchargement, les sites faisant l'apologie du terrorisme…), et en gardant une trace des actions effectués sur le réseau (logs), afin de pouvoir fournir les historiques en cas de besoin.

La CNIL autorise donc le filtrage de sites à caractère illégal (racistes, pédophiles, etc) mais également le blocage de n'importe quel site à caractère non productif, sans restriction à ce niveau. L'employeur peut interdire à ses employés de se rendre sur des réseaux sociaux, de télécharger des logiciels ou bien de consulter leur messagerie personnelle, il est cependant interdit à l'employeur de refuser de manière absolue l'utilisation d'Internet pour usage personnel à ses employés.

Il est bon de savoir également que consulter des données informatiques à l'insu de l'utilisateur peut être puni de 5 ans d'emprisonnement et de 300000€ d'amende (loi

d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011). De façon concrète, l'employeur ne peut pas consulter des mails, un dossier ou des fichiers indiqués comme « personnels ». Concernant les logs, le droit parle de « données relatives au trafic » ou « données de connexion ». La CNIL conseille donc de garder des fichiers de logs, comprenant au minimum l'identifiant de l'utilisateur, les date/heures de connexion et déconnexion. Ces logs doivent être gardés sur une période maximale de 6 mois. Ces logs peuvent également contenir les sites visités par l'utilisateur, ou les actions effectuées sur le système.

L'utilisateur doit dans tous les cas être informé des interdictions, des blocages et de la présence de filtrage sur le réseau de l'entreprise, ainsi que de ses droits d'accès et de rectification, de son droit d'opposition, des destinataires des données et des finalités poursuivies. Il est nécessaire de créer une charte informatique afin de consigner toutes les informations et règles nécessaires à l'usage de l'outil informatique, mais également téléphonique.

o La vidéosurveillance en entreprise

Il existe un autre point important sur lequel le chef d'entreprise doit apporter une attention particulière : la législation vis-à-vis de la vidéosurveillance. Pour faire au plus simple, pour respecter la loi, la vidéosurveillance doit avoir pour but la sécurité des biens ou des personnes et non la surveillance des employés, et ceux-ci doivent en être informé. Dans la pratique, de nombreux points sont à respecter. Notamment, une déclaration doit être déposée à la CNIL pour tout système de vidéosurveillance. Si ce système filme un lieu ouvert au public, il faut également faire une déclaration auprès du préfet du département. Les instances représentatives du personnel doivent également être informées avant la mise en place de caméras.

Exemple de panneau réglementaire :

Le dispositif doit aussi être indiqué par un panneau avec notamment le nom du responsable du système de vidéosurveillance. Le dispositif doit avant tout filmer des lieux de circulation (couloirs, entrées…) ou bien les lieux où de la valeur est stockée (entrepôts…), et

non le bureau d'un employé. Tout le monde n'a pas le droit de visionner les images. Une personne formée et habilitée doit être chargé de ce rôle, comme un responsable de la sécurité du site. Enfin, il y a une limite de durée de stockage des images, d'un mois.

La vidéosurveillance doit donc garder son rôle : pouvoir sécuriser un site, et utiliser les images en cas de vol ou de dégradation. Si le chef d'entreprise a bien compris ce rôle, et ne souhaite pas utiliser le système pour surveiller ces employés, les règles à respecter seront facilement assimilées.

UN PLAN DE SÉCURISATION DES DONNÉES

La sécurité passe avant tout par un plan de sécurité rédigé par le service informatique en charge de la maintenance du parc de la société. La sécurité englobe de nombreux principes, tels que la sécurité des mots de passe, la sécurité du matériel informatique, la sécurité des données… Il est important de n'oublier aucun de ces points, qui sont tous sensibles et peuvent conduire à de grandes conséquences en cas de défaillance.

Une entreprise cumule au fur et à mesure de son activité un grand nombre de données, c'est pourquoi il est nécessaire de les protéger et cela pour le bien de son activité. Selon une étude menée par le cabinet Vanson Bourne pour le compte d'EMC Corporation (Dell), publiée le 13/02/2015 sur le site « lepoint.fr », le coût des pertes de données intervenues en France l'an passé est évalué à 30,9 milliards d'euros, dont des coûts d'interruptions de services non planifiés, majoritairement dues à des pannes matérielles et logicielles, qui aurait quant à eux atteint 11 milliards d'euros.

La sécurité passe avant tout par la façon dont les outils informatiques fournis aux employés sont utilisés. Le meilleur antivirus en informatique c'est avant tout l'utilisateur, ses réflexes, sa bonne utilisation des outils ainsi qu'une connaissance de l'univers Web, qui est indispensable pour protéger au mieux les postes d'éventuelles attaques. Bien entendu, l'erreur est humaine et c'est pourquoi des systèmes de sauvegarde et de restauration de données « backup » sont mis en place par les services informatiques gérant le parc informatique d'une société. Les pertes de données peuvent avoir des conséquences très néfastes au bon fonctionnement économique des entreprises, c'est pourquoi notre société, Axolotl IT, met un point d'honneur à gérer efficacement vos données informatiques, avec un maximum de sécurité pour plus de sérénité, et en prévoyant chaque éventualité.

PLAN DE SÉCURISATION PAR AXOLOTL IT :

De quelle façon procédons-nous ?

- √ Sécurité des accès (identifiant/mot de passe)
- √ Confidentialité des données
- √ Stabilité des performances du système
- √ Intégrité des équipements (exemple : pas de matériel personnel en entreprise)

Pour maintenir la sécurité de l'entreprise, il est interdit :

- √ Toute installation ou téléchargement de logiciels ou pro logiciels sans consultation du service informatique.
- √ De connecter des périphériques externes non autorisés.
- √ De modifier les configurations d'origine

Cette sécurité est mise en place chez chaque collaborateur et il est nécessaire de respecter ce plan de sécurité afin de garder un parc informatique à jour et sécurisé pour le bien de l'entreprise.

o La sécurité en interne

La sécurité est un domaine très vaste, elle ne passe pas que par les identifications au système mais également par des habitudes à prendre comme verrouiller sa session (raccourci Windows + L) quand on s'absente de son poste même pour quelques minutes. Il faut aussi penser à attacher les postes portables via des câbles antivols (type Kensington). Il est également strictement interdit de connecter des périphériques auxiliaires extérieurs à l'entreprise et donc non sécurisés et potentiellement vulnérables.

Par exemple :

- √ Il ne faut pas brancher son téléphone personnel sur un poste professionnel même simplement pour le recharger.
- √ Il ne faut pas brancher de clef USB non professionnelle sur son poste.
- √ Il faut également prêter une attention toute particulière à l'ouverture des mails de type spams : s'ils sont rangés dans la boîte « courriers indésirables » c'est qu'ils peuvent éventuellement contenir des pièces jointes frauduleuses ou des virus.

C’est pourquoi la sécurité en entreprise est plus que primordiale, l’accès de l’ensemble des données est seulement attribué aux administrateurs du service informatique. L’IT doit également mettre en place un pare-feu pour repousser les intrusions sur les serveurs, et un antivirus sur les postes pour se prémunir contre les attaques venant d’Internet.

o Accès sécurisé par mot de passe :

La protection des données de l’entreprise et de chaque utilisateur passe également par la sécurisation des accès autrement dit des mots de passe. Un mot de passe doit respecter certains critères pour être totalement sûr. En plus du critère de nombre de caractères, il faut également respecter des critères « humains », comme ne pas communiquer son mot de passe à un collègue ou tout simplement ne pas le laisser écrit sur un post-it collé à l’écran.

Les critères qu’un mot de passe doit respecter, au minimum, sont les suivants :

- √ 8 caractères minimum, dont au minimum une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.
- √ Le mot de passe ne doit pas être intuitif, on ne doit pas pouvoir le deviner, de ce fait il ne doit pas correspondre à des distinctifs personnels.
- √ Il est possible de regrouper ces mots de passe dans un dossier fermé par mot de passe.

Les mots de passe types à éviter :

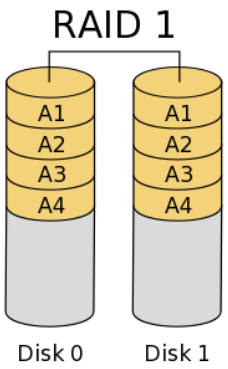
Password / motdepasse
123456 / azerty
changeme
F***y** (de même pour l’équivalent en français)
Michael (Microsoft déconseille, même en mémoire de la vedette défunte, de retenir « Michael » comme mot de passe.)

Les identifiants seront toujours transmis au nouvel arrivant par courrier à l’arrivée ou bien par mail, soit via un lien vers un générateur de mot de passe sécurisé soit via un mail

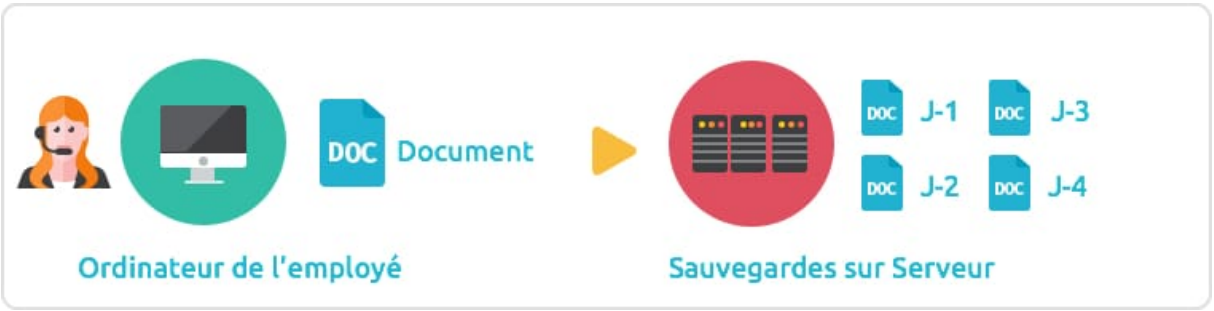
crypté. Toute demande concernant un mot de passe doit être faite à votre administrateur qui quant à lui n'a aucun droit de regard sur vos mots de passe.

o Mesures de sauvegarde des données :

Utilisation du RAID 1 : Le RAID 1 consiste à créer des copies miroir en temps réel des disques présents sur le serveur, les disques contiennent donc exactement les mêmes données au même moment. Les capacités de stockage dépendent directement du plus petit disque copié puisque le miroir ne pourra contenir plus que son ou ses antagonistes. Le raid 1 permet d'avoir au moins une défaillance s'il y a un miroir et plus s'il y a plusieurs miroirs.



La contrepartie étant que la moitié seulement de la capacité de stockage est utilisée, dans ce sens deux disques durs de 500 Go ne donneront que 500 Go de stockage et ainsi de suite. Le nombre de disques durs ne fait pas augmenter la taille maximum du stockage, cette limite d'utilisation est basée sur le plus petit disque dur. La sauvegarde des données est quant à elle assurée par une entreprise tierce chez qui nous louons des serveurs afin d'avoir une perte de données d'une journée maximum en cas de défaut (les sauvegardes sont effectuées tous les jours après 22h afin de limiter l'utilisation de bande passante pendant les journées de travail)



Ce système de sauvegarde permet à l'employé de garder ses documents en sécurité et de sauvegarder chaque modification de fichiers sur le serveur. Ainsi, même si un poste se fait

attaquer, aucun fichier ne sera perdu, et en cas d'absence de la personne travaillant sur un dossier important, un autre employé pourra prendre le relai et finir le travail sans encombre.

o Sécurité "physique" du matériel

Les locaux hébergeant le centre de sauvegarde et donc les copies des données de toute l'entreprise sont d'une importance critique, en effet si quoi que ce soit arrive aux données c'est l'entreprise entière qui en serait touchée. De ce fait une attention toute particulière doit être apportée en termes de consignes et de sécurité pour éviter les problèmes, qu'ils soient matériels, naturels ou même humain.

√ **Comment éviter les problèmes matériels ?**

Les problèmes matériels peuvent se révéler graves, car une intervention dessus pourrait nécessiter l'arrêt des services, qui même si celui-ci est temporaire est inenvisageable.

Pour pallier à ce problème l'entreprise effectue des maintenances de type préventive à intervalle régulier de deux ans : tous les deux ans le centre de sauvegarde est donc inspecté tout en étant toujours en fonctionnement. Ce travail d'orfèvre a jusqu'à ce jour permis d'éviter toute intervention de type curative.

Pour parvenir à la meilleure continuité de service possible, il est également nécessaire d'utiliser un onduleur afin au minimum d'avoir le temps d'éteindre correctement les services en cas de coupure de courant, et ainsi éviter des pertes de données sur les postes, par exemple, et au mieux permettre de continuer à utiliser les postes et services pendant une période, si l'onduleur le permet. Il est aussi possible d'utiliser des générateurs de secours.

√ **Comment éviter les problèmes de type naturel ?**

Par naturel nous entendons dégâts des eaux, tremblements de terre, incendies etc …

Les dégâts des eaux par exemple peuvent survenir de bien des manières, que ce soit une inondation de la ville où se trouve le centre de données à une fuite de canalisation dans le centre. Quoiqu'il en soit, pour prévenir ce type de désagréments quelques solutions simples existent et sont employées.

Une surélévation des matériels à risque est conseillée, afin d'éviter que ceux-ci soient touchés en cas de fuite. Il s'agit par exemple de le surélever par rapport au sol à l'aide d'une dalle de béton armé. Ces mêmes surélévations peuvent créer également un cheminement où l'eau

sera dirigée vers des bouches d'évacuation. Pour pallier à la fuite en elle-même des systèmes de détecteurs de fuites peuvent être utilisés afin de pouvoir localiser et donc intervenir très vite sur les lieux de la fuite. Des tubes hermétiques peuvent également être utilisés pour le cheminement de l'électricité et de l'ensemble des câbles, afin d'éviter tout risque de court-circuit. Le matériel à risque peut quant à lui être protégé par des baies d'indice de protection 66 (IP66), voire IP67 pour supporter une immersion temporaire.

√ **Comment éviter les risques liés à la chaleur ou au feu ?**

Dans un centre, la chaleur est un problème récurrent car la multitude de matériel informatique rassemblé dans une même pièce crée un échauffement conséquent. De ce fait le centre est entièrement climatisé afin de maintenir une température ambiante de 20°C en permanence. Des détecteurs de fumée et de chaleur sont installés aux endroits critiques, ils permettent d'indiquer si de la fumée se propage ou si la chaleur augmente de manière significative. Si un incendie se propage, il n'est bien sûr pas conseillé d'utiliser de l'eau sur du matériel informatique, un système au gaz sera donc bien plus adapté, afin de diminuer le taux de dioxygène dans la pièce, ce qui aura pour effet d'étouffer le feu par manque d'oxygène.

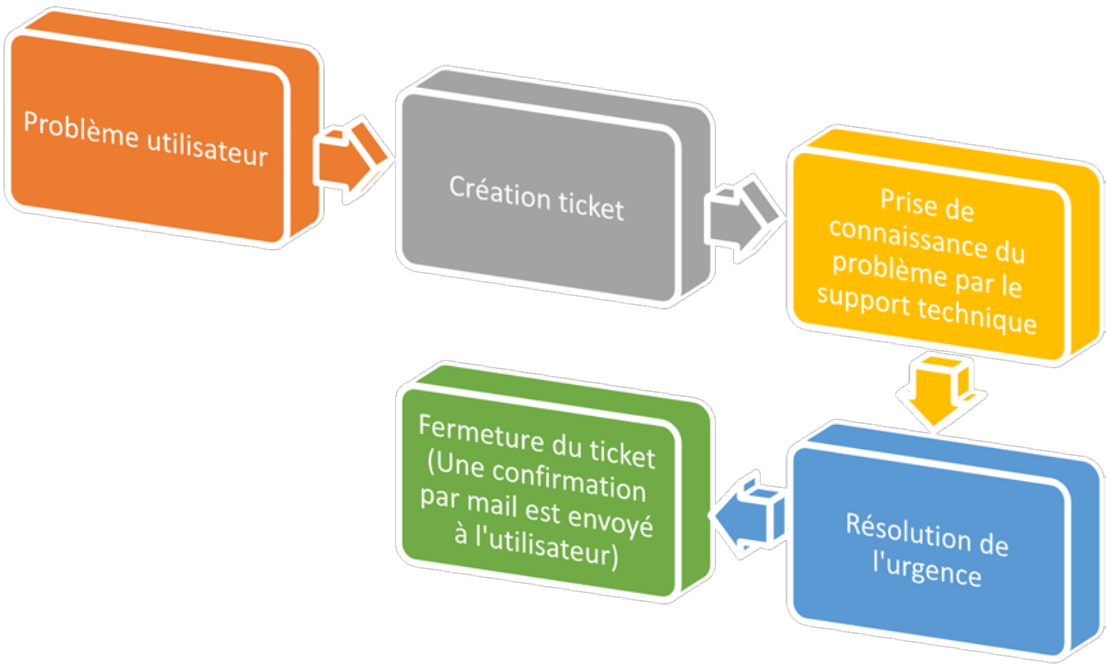
√ **Le facteur "humain".**

Bien évidemment, pour se protéger du "facteur humain", le centre doit être soumis à accès réglementé, notamment à l'aide de badges et digicodes, de caméras de surveillance, ainsi que d'alarmes pour contrer toute tentative d'intrusion.

o Sécurité des données numériques.

L'entreprise met à disposition des ressources informatiques comme des logiciels ou progiciels qui sont référencés au catalogue des logiciels autorisés, certains de ces logiciels peuvent être soumis à licence et donc à contrôle du nombre d'utilisateurs. L'entreprise fournit également un système d'exploitation déjà installé sur les postes, il est interdit d'en changer ou de le modifier sous peine de sanction. Pour toute demande de logiciel spécifique, il faut en référer au responsable de service qui fera une demande à la section compétente. Si le logiciel reçoit l'approbation du service, il pourra alors être intégré au catalogue, dans le cas contraire il sera impossible de l'utiliser sous peine de sanction, dû à une éventuelle mise en danger du réseau et de l'entreprise.

Les demandes d'installation de logiciel non installé par défaut, tout comme les pannes ou problèmes utilisateurs passent par une application web qui permet d'envoyer une demande sous forme de ticket au support informatique.



3 types d'urgences sont répertoriés par niveaux : Moyen, Elevé, Urgent.

- √ Les tickets avec le niveau **Moyen** peuvent être résolus dans les 24 heures.
- √ Les tickets avec le niveau **Élevé** doivent être résolus dans les 8 heures.
- √ Les tickets avec le niveau **Urgent** doivent être résolus impérativement dans les 4 heures.

Concernant les données à proprement parler, il est nécessaire de réduire les risques de suppression ou modification de fichiers de façon non voulue ou malveillante. Pour cela, il est important de "classer" les utilisateurs par services, et attribuer des droits de lecture/écriture sur les dossiers en fonction de leur service. Ainsi, par exemple, un utilisateur du service Commercial ne pourra pas supprimer ou modifier, ni même ouvrir un fichier du dossier "Commun Marketing". Sur serveur Windows, tout cela peut se gérer simplement depuis l'Active Directory. Ce dernier permet également de suspendre le compte d'un utilisateur, de réinitialiser son mot de passe en cas d'oubli, et bien d'autres choses.

CHARTE QUALITÉ SERVICE CLIENT

Afin de vous garantir une qualité de service la plus satisfaisante possible, Axolotl IT s'engage sur différents aspects, notamment la continuité de service en cas de panne, le relationnel client ainsi que la sécurité et la productivité :

Continuité de service en cas de panne :

Le bon fonctionnement de la plupart des entreprises repose désormais essentiellement sur le système informatique. Si celui-ci est défaillant ou "à l'arrêt", c'est bien souvent l'ensemble des salariés qui se retrouve sans outil de travail. C'est pourquoi l'un des objectifs principaux d'Axolotl IT est de vous permettre d'avoir un système stable, non seulement avec un minimum de pannes, mais également d'avoir un temps de panne le plus court possible, et avec des solutions immédiates pour garder un fonctionnement optimal. Pour cela, Axolotl IT s'engage à :

- √ Intervenir aussitôt en cas de problème. L'informatique est votre outil de travail, et il est de notre devoir d'intervenir rapidement en cas de panne.
- √ Proposer des solutions déployables rapidement en cas de panne, pour les équipements les moins coûteux.
- √ Privilégier une redondance des différents composants sur les serveurs afin d'avoir une continuité de service en cas de panne d'un composant (alimentation, switch…)

Relationnel client :

Nous estimons que la base même de toute entreprise fournissant des services est la communication. Nous nous devons de vous fournir un accès à toutes les informations pouvant vous être utiles, qu'il s'agisse de nos horaires ou bien de documentation informatique à destination de vos utilisateurs, et cela avec respect et efficacité. C'est pourquoi nous nous engageons à :

- √ Suivre un mémo interne pour les techniciens, afin de suivre les meilleures procédures possibles et de communiquer avec vous dans les meilleures des conditions.

- √ Mettre à votre disposition des questionnaires de satisfaction pour nous permettre d'améliorer la qualité de nos services et ainsi viser l'excellence.
- √ Vous informer sur la nature de l'intervention effectuée, et répondre à vos questions.
- √ Informer les utilisateurs sur les lois et règles appliquées dans l'entreprise au niveau de l'informatique.
- √ Faciliter la communication entre les utilisateurs et les techniciens, par l'utilisation de différents moyens de communication : téléphone, mail, outil de ticketing, de façon à ce qu'un technicien soit toujours présent pour répondre à l'utilisateur. Dans le cas contraire, nous nous engageons à vous recontacter rapidement.
- √ Avoir une bonne communication de manière globale : nous nous engageons à vous fournir un accès facilité à l'information, notamment les horaires, les questions générales, de la documentation sur les logiciels utilisés dans l'entreprise, les bonnes pratiques d'utilisation de l'outil informatique, tout cela accessible depuis notre site web ou bien depuis le réseau de l'entreprise.
- √ Conseiller les utilisateurs sur les bonnes pratiques d'utilisation de l'outil informatique, afin d'éviter les erreurs et donc améliorer la productivité de l'entreprise
- √ Établir des statistiques sur les services rendus par notre entreprise, afin de vous offrir un bilan détaillant les tâches que nous effectuons pour vous.

Sécurité et productivité :

Parce que vos données sont sensibles, et que notre rôle est de s'assurer que celles-ci sont protégées, nous avons décidé de nous engager afin de vous assurer la sécurité maximale. Notre raisonnement est simple : meilleure sécurité et fiabilité = moins de pannes et meilleure productivité.

Pour parvenir à réaliser ces objectifs, nous nous engageons à :

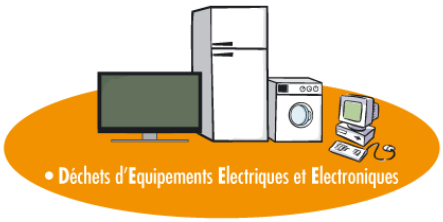
- √ Fournir du matériel de qualité reconnue afin d'avoir moins de pannes ou un temps plus long entre deux pannes.
- √ Fournir du matériel et des logiciels adaptés à l'utilisation prévue, afin que l'utilisateur ne soit pas bloqué par des limitations techniques
- √ Remplacer votre matériel ou logiciel défectueux par un matériel ou logiciel de qualité et performance équivalentes ou supérieures

- √ Effectuer un suivi et une gestion des stocks et du matériel, ainsi que du matériel de prêt, afin de savoir quel matériel est à quel endroit, et à qui, notamment par l'utilisation de QR Code sur chaque périphérique -> moins de perte de temps + de productivité pour des coûts faibles
- √ Entretenir le matériel régulièrement afin de prolonger sa durée de vie (nettoyage logiciel et matériel, suivi des plaintes des utilisateurs…)
- √ Garder un suivi des actions effectuées par notre service sur chaque poste ou pour chaque utilisateur afin d'avoir les bonnes informations, et ainsi nous permettre d'aider à améliorer la qualité des services rendus
- √ Garder à jour une base de données et un historique des problèmes rencontrés et de leurs solutions, afin de résoudre plus rapidement les problèmes récurrents
- √ Toujours chercher à améliorer l'existant, à optimiser, et non pas attendre que le système informatique soit dépassé pour agir
- √ Faire réaliser nos interventions par un personnel qualifié, formé, diplômé, avec de l'expérience et habilité à réaliser les interventions sur votre infrastructure
- √ Suivre et maintenir à jour un mémo interne comprenant des consignes et règles à destination des techniciens, afin de disposer d'une base solide et fiable pour effectuer les diverses opérations dans les meilleures conditions possibles
- √ Effectuer une veille technologique constante afin d'être au courant des dernières évolutions technologiques, et ainsi toujours garder un système informatique optimal, à jour et fiable
- √ Avoir une bonne communication implique également un suivi des tickets et des demandes des utilisateurs : cela implique donc une échelle d'importance basée sur des critères tels que : nombre d'utilisateurs impliqués, durée de la panne, impact de la panne sur le travail de l'utilisateur, possibilités de solutions dans l'attente de la résolution de la panne, etc.
- √ L'utilisateur doit donc être informé du suivi de son problème, et doit connaître les délais avant résolution de l'incident.
- √ Simplifier l'informatique pour les utilisateurs de manière générale, et ainsi améliorer la productivité, tout en évitant des erreurs d'utilisation
- √ Ne divulguer aucune information confidentielle. Les techniciens et l'ensemble de l'entreprise s'engagent à respecter la confidentialité des données des utilisateurs
- √ Fournir des logiciels et des licences valides et authentiques, ainsi que du matériel acquis de façon légale. Nous nous engageons à respecter la propriété intellectuelle.

- √ Suivre les bonnes pratiques pour améliorer la qualité des services informatiques, notamment en suivant les recommandations de l'ITIL. (Bibliothèque pour l'Infrastructure des Technologies de l'Information)

Dans un souci écologique mais également économique, nous nous engageons à :

- √ Gérer efficacement et intelligemment la récupération du matériel électronique usagé, notamment en réutilisant au maximum le matériel ou les composants en état de fonctionnement. (Également par l'utilisation d'équipements certifiés RoHS et la gestion efficace des DEEE, les déchets électriques et électroniques)
- √ Les déchets sont recyclés conformément aux normes françaises et européennes.



MEMO INTERNE

Pour chaque intervention le technicien d'Axolotl IT se doit de respecter des règles minutieusement pour véhiculer la meilleure image professionnelle possible. Le technicien doit prendre conscience qu'il représente la société, et que le client se fera un avis en se basant en grande partie sur son attitude générale. Afin d'aider le technicien dans sa démarche, nous tenons à insister sur les points suivants, qui doivent être respectés :

- √ Axolotl IT fournit des t-shirts à l'effigie de l'entreprise ainsi que des pantalons et des chaussures de sécurité à chaque nouveau technicien. Ce dernier devra pour chaque intervention porter ces tenues vestimentaires dans l'état qui lui a été donné et propre.

- √ Toute explication fournie par l'un de nos techniciens à l'utilisateur se doit d'être claire et limpide afin de ne pas perdre ce dernier dans un jargon informatique qui peut s'avérer parfois complexe pour une personne non-initiée.

- √ Vous devez écouter, conseiller et résoudre les problèmes de façon courtoise et aimable, en utilisant des termes informatiques appropriés afin de faciliter la compréhension de chacun.

- √ Vous devez être ponctuel lorsque vous fixez un rendez-vous. En cas de délai, informez l'utilisateur.

- √ Un système de tickets est mis à disposition des utilisateurs via une application web pour remonter les urgences et les problèmes rencontrés, ceux-ci sont directement envoyés sur la boîte mail des techniciens afin de les traiter le plus vite possible. Un suivi est alors effectué par la ou les personne(s) de l'équipe IT qui s'attribue(nt) le ticket et ce dernier ne doit être clôturé que lorsque le problème est résolu, ce qui enverra une confirmation de la résolution de la tâche par mail à l'utilisateur. Le technicien a également le devoir de tenir informé l'utilisateur de la progression du ticket.

- √ Toutes les demandes des utilisateurs seront traitées, cependant il est essentiel et nécessaire d'y apporter une certaine priorité selon les urgences afin de répondre au mieux aux attentes des utilisateurs.

- √ Aucune information confidentielle de nos clients ne doit être divulguée à un tiers, que ce soit au sujet de leurs documents de travail ou bien même de leurs mots de passe.

- √ Le matériel à disposition de l'utilisateur est avant tout configuré par notre service informatique pour contrôler au mieux l'éventuelle obsolescence du parc informatique et ainsi pouvoir anticiper les coûts futurs.

- √ Toutes nos licences logicielles sont contrôlées et renouvelées à la date d'échéance indiquée sur le contrat.

- √ Toutes applications et sites non productifs comme Facebook, MSN, Skype, Twitter, Instagram, et bien d'autres seront bloqués aux utilisateurs afin d'optimiser leurs temps de travail.

WEBOGRAPHIE

RoHS :
https://fr.wikipedia.org/wiki/Directive_RoHS

DEEE :
https://fr.wikipedia.org/wiki/D%C3%A9chets_d'%C3%A9quipements_%C3%A9lectriques_et_%C3%A9lectroniques

ITIL :
https://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

CNIL :
https://fr.wikipedia.org/wiki/Commission_nationale_de_l'informatique_et_des_libert%C3%A9s

Coûts des pertes de données :
http://www.lepoint.fr/high-tech-internet/pertes-de-donnees-la-facture-est-gigantesque-pour-les-entreprises-francaises-13-02-2015-1904888_47.php

Définition d'un RAID 1 :
http://www.mydiskmanager.com/raid0-raid1-raid5-jbod-cest-quoi-le-raid/

Schémas :
https://cours-informatique-gratuit.fr/cours/reseau-informatique-entreprise/

Les 5 mots de passes à éviter :
http://www.zdnet.fr/actualites/les-10-mots-de-passe-a-ne-surtout-jamais-employer-39711315.htm

Livre blanc juridique Olfeo :
https://olfeo.com

ANNEXE

TRAVAIL & DONNÉES PERSONNELLES

Les outils informatiques au travail

L'utilisation des outils informatiques s'est largement développée dans le monde du travail. Une utilisation personnelle de ces outils est tolérée par les tribunaux si elle reste raisonnable et n'affecte pas la sécurité des réseaux ou la productivité. C'est à l'employeur de fixer les contours de cette tolérance et d'en informer ses employés.

Le contrôle de l'utilisation d'Internet et de la messagerie : dans quel but ?

L'employeur peut contrôler et limiter l'utilisation d'internet (dispositifs de filtrage de sites, détection de virus…) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam »…)
Ce contrôle a pour objectif :
1. D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie…)
2. De limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux…).

Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.

À noter : Les marque-pages, « favoris » ou « bookmark » du navigateur ne constituent pas un espace personnel ou privé. Ajouter un site internet à ses « *favoris* » ne limite donc pas le pouvoir de contrôle de l'employeur.

Quelles garanties pour la vie privée ?

Les limites au contrôle de l'employeur

- L'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif.
- Les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite.
- Les logs de connexion ne doivent pas être conservés plus de 6 mois.

- **La protection des courriels personnels :**

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.
Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles.
Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :
- en précisant dans leur objet « Personnel » ou « Privé »
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « *mes documents* » ou dans un dossier identifié par les initiales de l'employé.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Édition octobre 2016 cnil.fr

Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages. En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé.

- **Les fichiers**

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement.
Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder :
- en présence de l'employé ou après l'avoir appelé
- en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprécier.

- **La communication des mots de passe**

Les identifiants et mots de passe (session Windows, messagerie…) sont confidentiels et ne doivent pas être transmis à l'employeur. Toutefois, si un employé absent détient sur son poste des informations indispensables à la poursuite de l'activité, son employeur peut exiger la communication de ses codes si l'administrateur réseau n'est pas en mesure de fournir l'accès au poste.

L'information des employés

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité.
Chaque employé doit être notamment informé :
- Des finalités poursuivies,
- Des destinataires des données,
- De son droit d'opposition pour motif légitime,
- De ses droits d'accès et de rectification.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service…

Quelle formalité CNIL ?

La mise à disposition d'outils informatiques sans contrôle individualisé de l'activité doit être déclarée à la CNIL (déclaration simplifiée de conformité à la norme simplifiée n°46 ou déclaration normale).
S'il existe un contrôle individualisé (analyse des relevés de connexion poste par poste, calcul du temps passé sur internet…), il faut procéder à une déclaration normale auprès de la CNIL.
Un système qui n'a pas fait l'objet d'une déclaration à la CNIL ne peut pas être opposé aux employés.
Si l'organisme qui a mis en place l'un de ces dispositifs a désigné un Correspondant informatique et libertés (CIL), aucune formalité n'est nécessaire auprès de la CNIL, le CIL devant les noter dans son registre.

Quels recours ?

En cas de difficulté, vous pouvez saisir :
- les services de l'inspection du Travail
- le procureur de la République
- le service des plaintes de la CNIL, sur les modalités de mise en œuvre d'un dispositif de contrôle de l'activité.

Les textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Articles L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-32 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
  Articles 226-16 et suivants (atteintes aux droits des personnes résultant des traitements informatiques)
- La loi du 6 janvier 1978
- **Délibérations de la CNIL**
  Norme simplifiée n°46

Voir aussi

Guide pour les employeurs et les salariés
- L'accès à la messagerie d'un salarié en son absence
- Peut-on accéder à l'ordinateur d'un salarié en vacances ?
- Le contrôle de l'utilisation d'internet et de la messagerie

Contact CNIL
Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur www.cnil.fr. Vous pouvez également appeler la permanence juridique de la CNIL au 01 53 73 22 22, du lundi au vendredi de 10h à 12h et de 14h à 16h.