AutoConcept

Étude avant-vente et sécurité informatique

NumiLor

Vos pensées, nos idées

FLORIAN LAMBERT

Technicien support à l'utilisateur chez NumiLor

Pour me contacter :

florian.lambert@numilor.fr

SOMMAIRE

1

SERVICE INFORMATIQUE

Analyse de l'existant et axes d'amélioration

210 000,00 €

Somme perdue suite à des défaillances techniques

QUOI CHANGER ?

Habitudes vis-à-vis de l'informatique
Organisation & communication
Qualités humaines & relationnelles

PROTÉGER LES DONNÉES

Ce qui est fait

Plantage d'un disque dur menant à d'énormes pertes financières

Ce qu'il fallait faire

Mettre en place une solution de sauvegarde

Ce qui est fait

Intrusion d'un client sur le poste d'une commerciale dépourvu de mot de passe

Ce qu'il fallait faire

Attribuer obligatoirement à chaque utilisateur une identité numérique définie par un mot de passe

Ce qui est fait

Un utilisateur se plaint du même problème depuis plusieurs mois

Ce qu'il fallait faire

Créer une solution de visualisation des demandes en cours avec un suivi sur l'état d'avancement

QUALITÉS HUMAINES ET RELATIONNELLES

Ce qui est fait

Absence d’explication des techniciens ou vocabulaire trop compliqué

Ce qu’il fallait faire

Faire preuve de pédagogie et d’empathie

2

SOLUTIONS TECHNIQUES

Sécurité des données et des postes de travail

Un système d'information doit être défendu en associant à chaque utilisateur dont l'identité sera vérifiée, des droits qui lui permettent d'accéder aux ressources qui lui sont utiles pour travailler et uniquement celles-là.

POLITIQUE DES MOTS DE PASSE

Force brute

...

aaaaaa9

aaaaaa0

aaaaaaA

aaaaaaB

...

Phishing

Une activité suspecte a été détectée sur votre compte : veuillez vous identifier

Vol de masse

Fuites de détails personnels de la part de géants du web (Yahoo, PlayStation, etc...)

POLITIQUE DES MOTS DE PASSE

Statique

+ Temporaire
+ Nombre d'essais
+ Longueur et variation des caractères

Dynamique

+ A usage unique
+ Renouvellement permanent
+ Utilise un boîtier ou une application mobile

Biométrique

+ Presque inviolable
+ Cher/compliqué à mettre en place
+ Dépend de facteurs externes

Caractères	Combinaisons
(a-z)	**208 827 064 576**
(a-z + A-Z + 0-9 + &-@)	**2 044 140 858 654 976**

Tableau d'étude de la robustesse d'un mot de passe statique de 8 caractères

SAUVEGARDE DES DONNÉES

En interne ou en externe ?

Question du coût : matériel & entretien
Question de l'aspect matériel des données

Sur quel(s) support(s) ?

Disques durs
Bandes magnétiques
Cloud

Vérification des données ?

S'assurer qu'elles sont correctes et aptes à fonctionner en cas de panne

SÉCURITÉ DES POSTES DE TRAVAIL - CÔTÉ TECHNIQUE

Protections contre l'extérieur

+ Pare-feu
+ Antivirus
+ Mises à jour
+ Cryptage des données

Droits des utilisateurs

+ Installation de logiciels
+ Modification de fichiers et exécution de commandes avancées

SÉCURITÉ DES POSTES DE TRAVAIL - CÔTÉ HUMAIN

Surveiller son matériel

+ Eviter les vols
+ Eviter les pertes

Prendre garde aux supports de stockage inconnus

+ Répandre un virus sur le réseau
+ Installer un processus siphonneur
+ Installer un logiciel espion

Naviguer sur internet et en déjouer les pièges

+ Télécharger à partir de sources sûres
+ Reconnaître une tentative d'hameçonnage
+ Oser demander de l'aide si besoin

AUTO CONCEPT

Analyse de l'existant et axes d'amélioration

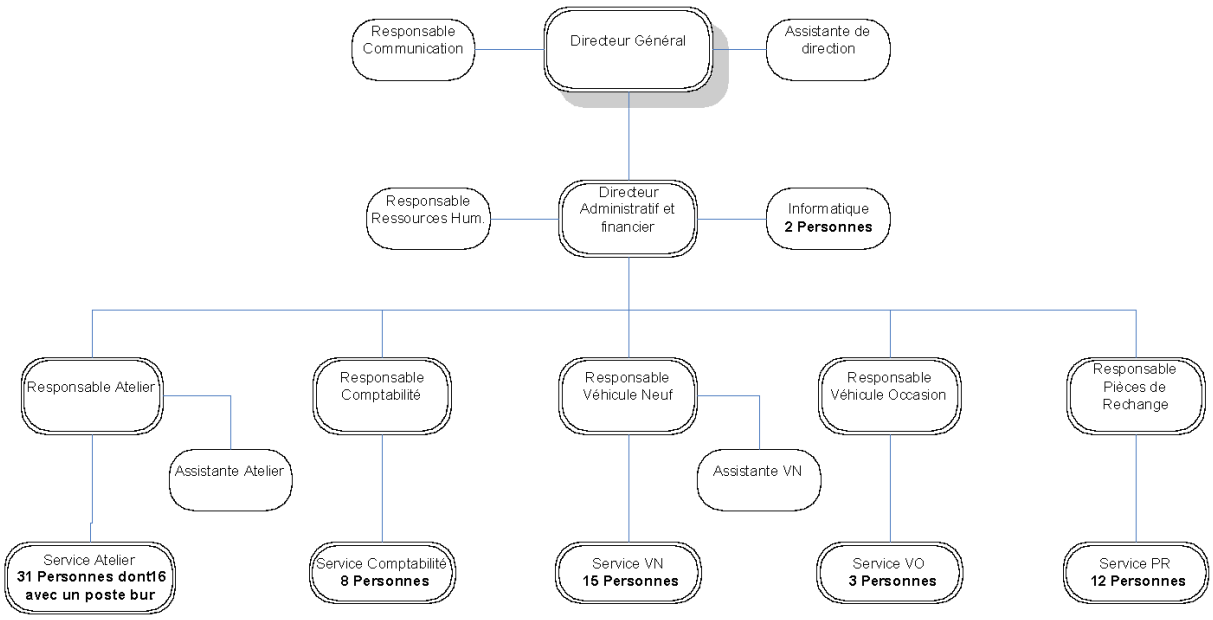
Sécurité des données et des postes de travail

Sommaire

Qui sont les acteurs ?

AutoConcept

Organisation



AutoConcept est une entreprise de vente de véhicules neufs et d'occasions. Elle en assure la maintenance et son équipe est composée de 83 personnes. Son parc informatique est composé de 68 machines.

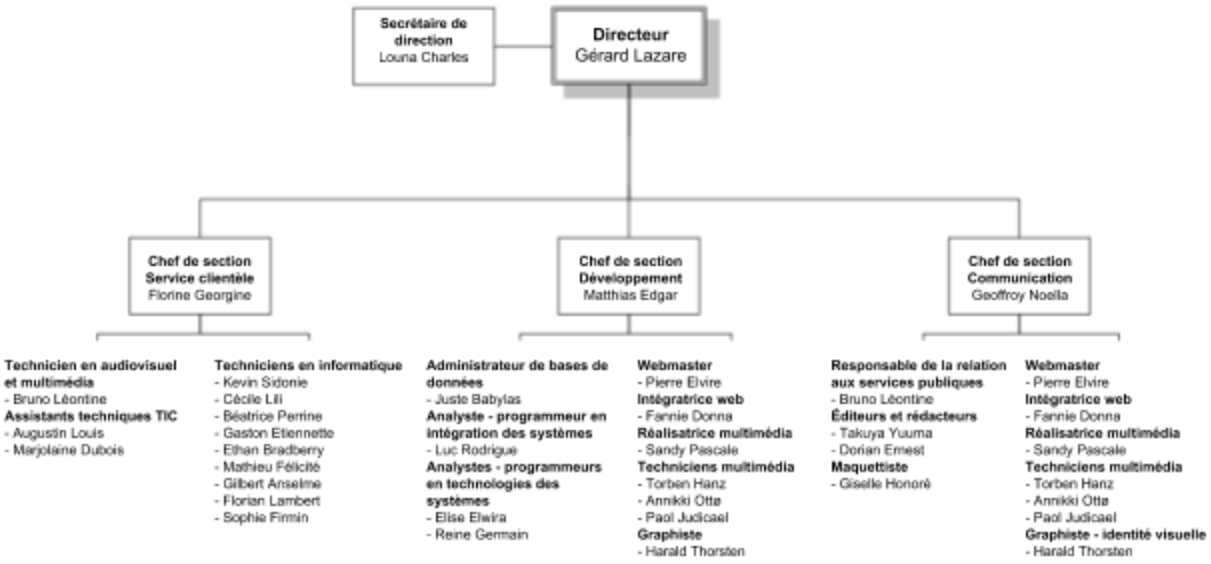
Appel d'offres

Elle souhaite externaliser les prestations informatiques réalisées jusqu'à présent en interne, par deux informaticiens.

NumiLor

Présentation de l'entreprise

NumiLor est une société de services informatiques à responsabilité limitée au capital de 320 000 euros. Dirigée par Gérard Lazare depuis sa création en 2008 à Nancy, elle compte 39 membres et exerce les métiers d'éditeur de logiciel, d'installateur de réseau informatique d'entreprise, de gestionnaire en maintenance informatique et propose une offre de formation aux nouvelles technologies de l'information, de création de sites internet et autres projets multimédia.



Analyse de l'existant

Service informatique

Rapport du service commercial

AutoConcept a choisi d'amortir son matériel sur 3 ans. La chef comptable ne souhaite pas renouveler son matériel avant la fin de la période d'amortissement. Cette donnée n'impacte pas la qualité du matériel et des interventions effectuées par les deux informaticiens de l'entreprise. Ce rapport fait état des faits suivants, qu'on peut classer en trois catégories :

Compétences des informaticiens

Savoir protéger les données

Savoir-faire

- Lenteur de certains postes,
- Crash disque du poste d'un commercial : perte d'exploitation 150 000 euros,
- Intrusion d'un client sur un poste d'une commerciale dépourvu de mot de passe,
- Messages intempestifs de « version de Windows pirates »,
- Un utilisateur du service commercial se plaint que son poste, après plusieurs séjours au SAV, présente toujours les mêmes symptômes,
- Un utilisateur de la comptabilité soupçonne le SAV d'avoir consulté des documents confidentiels sur son poste lors d'une intervention. Ces informations ont été divulguées à des tiers.

Organisation du travail et communication au sein de l'entreprise

Savoir s'organiser

Savoir communiquer sur les actions menées

- Délais d'intervention : un poste d'une secrétaire commerciale est parti en SAV durant 2 jours. Elle n'a pas pu terminer un document pour conclure une affaire. Perte : 60 000 euros,

- Un utilisateur de l'atelier rapporte qu'il a dû insister auprès du service informatique pour retrouver son écran d'origine. Un écran plus petit lui avait été remis après une intervention,
- Un utilisateur du service VO se plaint depuis plusieurs mois d'avoir des problèmes avec sa souris. Personne n'a répondu à son problème,
- Une bonne partie des utilisateurs se plaignent de voir leurs postes partir en SAV sans savoir quand il reviendra.

Qualités humaines et relationnelles

Savoir-être

Savoir transmettre les bonnes pratiques

- Tenue des informaticiens : « un matin, l'un d'eux est arrivé en jogging pour dépanner un poste alors qu'un commercial était avec un client ». Un autre a répondu de manière déplacée à la demande d'un utilisateur de le dépanner,
- Attitudes des techniciens : absence d'explication sur les interventions, ou parfois discours trop techniques,
- Plusieurs utilisateurs se plaignent de l'accueil téléphonique du service informatique,
- Un utilisateur signale que son MSN ne fonctionne pas et souhaite que son poste soit réparé rapidement. (NB : la direction a demandé au service informatique de bloquer MSN. Depuis la productivité a considérablement augmentée).

Axes d'amélioration

Les techniciens de ***NumiLor*** qui interviennent dans la maintenance de postes informatiques pour nos clients travaillent d'une autre manière. Les aspects relatifs à la protection des données et des postes de travail seront abordés dans la partie "*Solutions techniques*" disponible en page 9. Pour chaque catégorie précédemment explicitée, nous allons présenter les solutions que nous avons mis en place afin d'offrir le meilleur service possible.

Compétences des informaticiens

La lenteur d'un ordinateur peut se situer à plusieurs niveaux et peut être causée par différentes causes. L'utilisateur normal peut utiliser le terme "lenteur" pour décrire un ralentissement de la machine, par exemple des programmes qui mettent un temps anormal à se lancer, du texte tapé au clavier qui apparaît quelques secondes plus tard ; ou une lenteur du réseau, si le débit n'est pas suffisant pour télécharger une vidéo ou un fichier ou si la session met cinq minutes pour démarrer et se configurer. C'est au technicien informatique de détecter la

raison de ces ralentissements et d'y remédier.

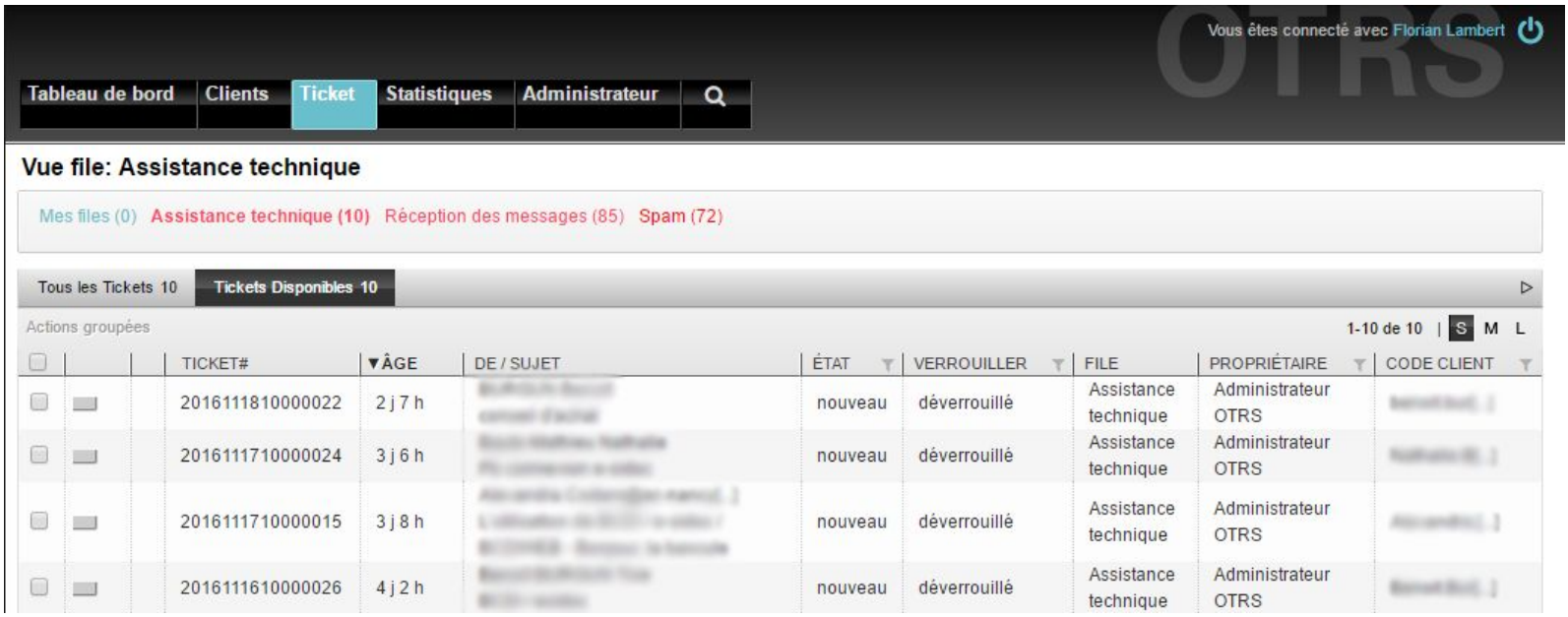
Le service informatique dispose d'un budget qui doit lui permettre d'acheter du matériel en quantité suffisante ainsi que des licences professionnelles. Lors d'une masterisation (clonage d'ordinateurs pour une installation rapide d'un parc informatique), il se peut que la version de Windows donne lieu à un message stipulant que sa version n'est pas authentique. Si les licences ont bien été achetées, il suffit de réinstaller les fichiers de licence ou de réinitialiser l'état de cette dernière. Une procédure détaillée est disponible dans les références de ce document.

En revanche, s'il s'agit de versions non légitimes de Windows, l'entreprise encourt des risques juridiques (amende de plusieurs dizaines de milliers d'euros et peine de prison) et techniques (cheval de Troie, virus, etc…). Il faut faire les choses proprement et installer sur l'ensemble des machines concernées une vraie version du système d'exploitation obtenue auprès de Windows en utilisation le droit de "reimaging". Il permet de reproduire une image tant que les copies sont identiques au produit original.

Un poste envoyé au service après-vente doit en ressortir comme neuf. Selon le rapport du service commercial, un ordinateur qui a été pris en charge à plusieurs reprises par le SAV est toujours défectueux. C'est un problème qui ne devrait pas se produire. Avant de rendre la machine à son propriétaire, elle doit subir une batterie de tests en fonction de ce qui a été réalisé sur elle. Prenons le cas d'un ordinateur portable : si le clavier possède des touches qui ne répondent pas et que ce dernier est changé par un clavier du stock qui est neuf mais déballé et à l'air libre, il peut être judicieux de le nettoyer de sa poussière et de le tester avant de rendre l'ordinateur. Durant le passage au SAV de l'ordinateur, il faut bien évidemment prêter une machine de rechange à la personne qui vient déposer la sienne.

Organisation du travail et communication au sein de l'entreprise

Les demandes d'interventions sont formulées par un système de tickets. Nous utilisons la plateforme OTRS pour sa capacité à pouvoir gérer plusieurs membres (nos techniciens) qui vont s'occuper en fonction de leurs emplois du temps des demandes en cours. L'interface est simple, les tickets sont ordonnés chronologiquement, un état ouvert ou fermé leur est attribué et il est possible de les annoter pendant l'intervention afin de tenir un suivi de l'état d'avancement. Si nous recevons une demande par téléphone ou courriel ne passant pas par la plateforme, nous créons manuellement le ticket pour répondre à un besoin de traçabilité et offrir la possibilité à l'un de nos techniciens de le prendre en charge.



Liste des tickets reçus et toujours ouverts

Lorsqu'une personne travaille sur une intervention, elle est présente du début jusqu'à la fin. Elle peut faire appel à un collègue si la situation s'y prête. Ce suivi assure à notre client un service personnalisé et maîtrisé. Nous répondons aux demandes dans la journée grâce à Florine Georgine, chef de section au service clientèle. Elle s'occupe de la réception principale des tickets et les redistribue dans différentes files d'attente (intervention en interne, en externe, animation d'une session de formation, etc…) et nos techniciens reçoivent sur leurs téléphones portables une notification immédiatement lorsqu'un ticket est affecté à leur domaine d'intervention.

Nous apprécions le contact téléphonique avec nos clients afin de limiter les délais qu'impose un échange par courriel. Cependant, nous utilisons toujours ce dernier moyen pendant nos interventions : il permet de prévenir par écrit de la date d'opération, de la manière dont elle va se dérouler, de ce dont le technicien pourrait avoir besoin comme données ou matériels ; et d'obtenir un retour du client sur la résolution de son problème. Ces échanges par courriel sont stockés dans la plateforme de tickets lorsque ce dernier est clos.

Au sein de ***NumiLor***, nos interventions sont moins nombreuses mais nous conservons un fonctionnement similaire : notre intranet possède un formulaire de contact que reçoivent nos deux assistants techniques. Ils résolvent le problème dans l'heure pour permettre à nos collaborateurs de poursuivre leur travail sans perte de temps. S'il s'agit d'un problème matériel, nous possédons un stock régulièrement mis à jour pour nous mais également nos clients.

Qualités humaines et relationnelles

Le technicien de maintenance, lorsqu'il effectue une opération auprès d'une personne, peut se limiter à réparer le problème et s'en aller, c'était souvent le cas chez ***AutoConcept***. Ce mode de fonctionnement pose plusieurs problèmes : la personne qui rencontre le problème ne sait pas d'où il vient ou comment il a été résolu. A l'avenir, si la situation se reproduit, le technicien devra se rendre sur place une fois de plus pour le même problème et ainsi de suite. Le client peut se trouver frustré par cette situation à laquelle il est totalement impuissant.

Une autre approche existe quant aux interventions de ce type : la pédagogie. Nous pensons qu'un bon technicien est d'abord un bon pédagogue. Depuis notre implantation à Nancy, nous avons fonctionné de la manière suivante : lorsque nous intervenons pour résoudre un problème que ce soit en interne ou en externe, nous avons pour objectif de faire en sorte que la personne qui a sollicité notre aide sache pourquoi le problème est apparu, comment le résoudre et quelles sont les bonnes attitudes à avoir pour éviter qu'à l'avenir il survienne de nouveau. Le fait d'apprendre à l'utilisateur les bons usages de son poste de travail, ce qu'il peut faire et ne pas faire, comme l'utilisation de messageries instantanées non professionnelles, fait également partie de la mission du technicien. Cette démarche pédagogue permet à nos clients de gérer eux-mêmes la situation. Nous constatons qu'ils nous sollicitent rarement pour le même problème, cela nous donne l'opportunité d'élargir notre clientèle sur le bassin nancéien tout en conservant une quantité de travail identique.

La présentation et le contact humain est un facteur clé dans le monde de l'entreprise. Les informaticiens en font part et ne peuvent déroger à la règle. D'une manière générale, leur position ne leur impose pas de porter un costume. Une chemise et/ou un pull, un pantalon et des chaussures de ville s'harmonisent très bien ensembles. Il faut éviter les vêtements trop détendus comme les joggings, les couleurs flashies ou les flocages de grande taille.

La ligne téléphonique du service informatique n'est pas à négliger. L'utilisateur qui appelle est confrontée à un problème et c'est à la personne qui décroche le téléphone que revient la tâche de la rassurer sur le fait que sa demande a été comprise et sera traitée dans les plus brefs délais. Voici une procédure à guise d'exemple qui fonctionnerait chez ***AutoConcept*** : décrocher le combiné, annoncer que la personne est bien au service informatique, l'inviter à présenter sa demande, l'écouter activement, reformuler son problème, lui demander dans quel bureau elle se trouve si on ne le sait pas déjà et lui annoncer une date à laquelle un technicien viendra s'occuper de sa situation.

Solutions techniques

La problématique de la sécurité

Le système d'information (SI) fait partie intégrante de l'entreprise. Il peut avoir plus ou moins d'importance selon le secteur d'activité de cette dernière mais dans le cas d'***AutoConcept***, la plupart des employés disposent d'un poste de travail et s'en servent quotidiennement pour des tâches variées telles que la gestion des stocks, le publipostage ou le calcul de la trésorerie. Les menaces extérieures sont nombreuses : perte d'argent due à un détournement ou une indisponibilité du SI, perte de crédibilité comme en 2004 où des malfaiteurs en Suède se sont appropriés les adresses e-mail de plusieurs entreprises et les ont menacé de diffuser du contenu pornographique à leurs clients si elles ne leurs versaient pas 7 000 euros. Afin de palier contre ces problèmes, nous pouvons développer une protection sur deux axes : la sécurisation des données et des postes de travail.

Sécurité des données

Politique des mots de passe

Un système d'information doit être défendu en associant à chaque utilisateur dont l'identité aura été vérifiée au préalable, des droits qui lui permettent d'accéder aux ressources qui lui sont utiles pour travailler et uniquement celles-là.

Risques

Les pirates disposent de tout un arsenal pour subtiliser des mots de passe et pénétrer dans une boîte mail professionnelle par exemple.

Force brute

La plupart des mots de passe sont simples : "123456", "azerty", etc… En forçant avec des outils facilement téléchargeables tels que Sentry MBA qui permettent de faire des milliers de tests d'authentification sur un site en mixant un identifiant et un mot de passe, on peut aisément trouver la bonne combinaison et voler le compte.

Phishing

Un mail frauduleux demande à la personne d'entrer ses identifiants de connexion suite à une activité suspecte découverte sur son compte. Cette méthode simple se déjoue aisément quand on sait décrypter les erreurs mais sur un énorme nombre d'envoi, de nombreuses personnes tombent dans le piège.

Vol de masse

Le piratage de Yahoo en septembre 2016 de quelques 500 millions de comptes permet aux pirates de tester leurs informations volées sur d'autres sites puisque plus de 60% des personnes utilisent un même nom d'utilisateur et mot de passe pour plusieurs de leurs comptes.

Solutions

Mot de passe statique

C'est la méthode la plus courante en informatique et la plus simple à mettre en place. Il faut choisir les règles de sécurité que l'on souhaite associer à ce mot de passe :

- Sa durée de validité : un changement fréquent peut se faire avec une vérification quant au nouveau mot de passe afin qu'il ne soit pas le même qu'un précédant utilisé six mois avant,
- Le nombre d'essais autorisés : si par exemple au bout de 3 essais le mot de passe est invalide, on peut verrouiller le compte pour empêcher une attaque par force brute,
- La longueur de la chaîne de caractères : plus elle est longue, plus le mot de passe solide,
- Les types de caractères utilisés : mélanger minuscules, majuscules et caractères spéciaux est une excellente solution qui renforce la force du mot de passe.

Longueur de la chaîne	Caractères utilisés	Combinaisons possibles
8	(a-z)	**208 827 064 576**
8	(a-z + 0-9)	**2 821 109 907 456**
8	(a-z + A-Z + 0-9)	**218 340 105 584 896**
8	(a-z + A-Z + 0-9 + &-@)	**2 044 140 858 654 976**

Tableau d'étude de la robustesse des mots de passe

Mot de passe dynamique

Jetable et à utilisation unique, il change en permanence. L'utilisateur utilise un petit boîtier qui génère un code ou bien une application mobile. Cette solution est bien plus sécurisée que la précédente mais a le défaut de demander plus d'actions de la part de l'utilisateur et peut devenir lourd pour ce dernier.

Mot de passe biométrique

Seule une personne possède ce mot de passe ce qui le rend plus sécurisé. Il peut être digital, oculaire, vocal ou encore facial. Ces méthodes sont sujettes à la qualité des capteurs, au fait que l'utilisateur ne présente pas de blessure au doigt ou encore que sa rétine ne soit pas trop éloignée du lecteur. Elles requièrent l'installation d'un matériel adéquat qui peut engendrer un coût supplémentaire.

Sauvegarde des données

La volumétrie des données que l'on souhaite préserver est le premier critère à prendre en compte lorsque l'on prévoit de sauvegarder des données. Lors de cette procédure, il peut également être utile de cibler ce qui doit être enregistré : inutile de copier à chaque fois une donnée qui ne change jamais, cela implique une perte de temps et d'énergie. L'entreprise doit définir la fréquence de sauvegarde qu'elle souhaite définir : si elle l'effectue toutes les 24 heures, elle doit être capable d'assumer de perdre dans le pire des cas une journée de travail. Selon ses activités, elle peut augmenter cette fréquence mais cela implique une charge supplémentaire du matériel de sauvegarde et une augmentation de l'énergie consommée.

Où sauvegarder ?

Des contraintes budgétaires amènent souvent les entreprise à externaliser leur solution de sauvegarde, réalisée par un tiers sur ses serveurs. Elle ne pourra pas maîtriser en totalité sa politique de sauvegarde. Elles peuvent également choisir d'internaliser ce processus ce qui leur donnera un contrôle totale sur la manière dont elles veulent effectuer la sauvegarde. Cette solution implique un investissement en amont de la part de l'entreprise quant au matériel.

Quel support pour stocker ?

Le disque dur est en concurrence avec la bande magnétique qui offre des performances compétitives grâce à sa capacité et sa longévité. Ces médias sûrs peuvent être placés dans un coffre-fort et déplacés aisément. De part leur construction, les bandes sont plus résistantes aux chocs que les disques durs. Ces dernières années ont vu l'apparition d'une méthode de stockage dématérialisée : le Cloud. Les offres sont nombreuses, de la gratuité à près de 5,64 euros par giga octet de donnée. On élimine le coût de l'achat du matériel et de son entretien

mais on perd le contact physique ce qui justifie un prix est plus élevé que les deux solutions précédentes.

Vérifier les données

Endormies sur leurs supports, il était jusqu'à présent difficile de vérifier l'intégrité des données puisqu'il faut posséder une reproduction de son infrastructure informatique pour les tester. Des solutions de virtualisation telles que Veeam offrent la possibilité de virtualiser un environnement de travail sur lequel on peut tester la qualité des sauvegardes réalisées et s'assurer qu'en cas de problème, on pourra les utiliser pour restaurer le système.

Sécurité des postes de travail

L'ordinateur ne peut pas fonctionner sans utilisateur. C'est ce lien homme/machine qui doit nous faire comprendre que lorsqu'on parle de sécurisation d'un ordinateur, il faut également apprendre à la personne qui s'en sert les gestes à adopter afin de garantir leur sécurité et celle de leurs données.

Sécurité technique

Combiné à la sécurisation des données par une sauvegarde quotidienne, l'administrateur d'un réseau peut le protéger des accès non sollicités en provenance d'internet à l'aide d'un pare-feu. Sur le poste de travail, un anti-virus complète son travail tout en veillant à ce qu'il soit mis à jour régulièrement afin de pallier aux failles de sécurités qui apparaissent avec le temps. L'administrateur du réseau a la possibilité de désactiver ou interdire l'installation de programmes inutiles quant au bon fonctionnement de la machine. Parfois de sources inconnues, ils représentent une porte d'entrée dans la sécurité de l'environnement informatique.

Le côté numérique présente de nombreuses brèches à combler mais il en est une qui se moque de toutes les précautions précédentes : le vol et la perte. Les dispositifs sont de plus en plus petits (tablettes, ultrabook, smartphone, carte SD, etc…) et doivent être protégés. Si un appareil de ce type venait à disparaître, des données confidentielles relatives aux activités de l'entreprise, des fichiers clients ou encore des plans prévisionnels pourraient tomber entre de mauvaises mains : l'utilisateur a pour mauvais réflexe de sauvegarder ses mots de passe pour accéder plus vite à son travail. Pour protéger les appareils sensibles à la perte ou au vol (clés USB, disques durs, etc…), on peut les crypter avec des logiciels dédiés comme truecrypt ou Axcrypt. Il existe également des clés USB auto-chiffrantes.

Former l'utilisateur

Avant de s'en remettre à utiliser la cryptographie, il y a des gestes préventifs que tout le monde peut adopter afin d'éviter de perdre son matériel :

- Ne jamais laisser son matériel sans surveillance,
- Fermer à clé son bureau,
- Attacher avec un câble son ordinateur portable.

Il faut savoir que les clés USB sont un vecteur de la propagation des virus qui se répandent une fois branchés à un poste de travail. Certains en siphonnent le contenu à l'insu de l'utilisateur. Il est préférable d'utiliser une clé personnelle dont l'origine et le contenu sont de confiance. Cette règle s'applique aussi aux autres supports amovibles tels que les disques durs ou les cartes mémoire. L'idéal est de posséder une clé pour l'usage personnel est une pour l'usage professionnel.

C'est bien connu, un employé utilise souvent son poste professionnel pour répondre à des fins personnelles et c'est à ce moment là qu'on peut se retrouver sur un site malveillant qui pourrait utiliser les failles du navigateur pour récupérer les données présentes sur la machine. Plutôt que de simplement interdire à l'utilisateur de télécharger un programme, il peut être plus judicieux de lui expliquer quels sont les risques qu'il encourt et fait encourir à l'entreprise en installant un programme dont l'origine est inconnue. Voici quelques actions à garder en tête :

- Apprendre à l'utilisateur à reconnaître un site sécurisé : certificat SSL, URL légitime…,
- Savoir télécharger le bon logiciel : nature de l'éditeur, site de provenance du téléchargement...,
- Les données relatives au fonctionnement de l'entreprise ne doivent être mises en ligne (dans le cadre d'un travail collaboratif par exemple) que sur une plateforme qui aura été validée par l'entreprise,

Nous avons parlé de phishing en page 10, cette méthode mise sur la crédulité de la personne qui va lire le message, souvent sous la forme d'un e-mail. En observant l'adresse de l'expéditeur, l'orthographe, le caractère urgent du message ou encore une pièce jointe suspecte, on peut facilement en conclure sur le caractère frauduleux de ce courriel. Il ne faut pas hésiter à se défaire des messages suspects : l'adresse e-mail d'un collaborateur peut avoir été subtilisée pour gagner la confiance de sa liste de contact.

Afin de faire en sorte que l'utilisateur ne se sente pas seul face à tous les problèmes qu'il peut rencontrer tous les jours, il faut lui faire comprendre que lorsqu'il est confronté à une situation suspecte, il peut alerter le support informatique. En réagissant vite et en faisant remonter ce type d'incident à la hiérarchie, on peut empêcher une attaque qui vise l'entreprise entière ou même plusieurs (hébergement mutualisé des données).

Bibliographie

WikimediaImages. Free vector graphic: Car, Rental, Icon, Key. [En ligne]. Publié le 12/08/2015. [Consulté le 15/11/2016]. Disponible : https://pixabay.com/en/car-rental-icon-key-automobile-872717/

Elionas | Free illustration: Pear, Icon, Light, Seem, Button | [En ligne] | Publié en juin 2016 | [Consulté le 14/11/2016] | Disponible : https://pixabay.com/en/pear-icon-light-seem-button-1459382/

Kropekk_pl. Free illustration: Incandescent, The Light Bulb, Icon. [En ligne]. Publié en août 2016. [Consulté le 14/11/2016]. Disponible : https://pixabay.com/en/incandescent-the-light-bulb-icon-1586297/

ILM Informatique. Activités de la société - ILM informatique. [En ligne]. Publié en 2008. [Consulté le 19/11/2016]. Disponible : http://www.ilm-informatique.fr/

Doc'Insa. Exemple de plan détaillé d'une partie présentant une entreprise. [En ligne]. [Consulté le 15/11/2016]. Disponible : http://docinsa.insa-lyon.fr/projet/diere/contenus/doc/presentation_entreprise.doc

Service-Public-Pro. Créer une société - professionnels. [En ligne]. Vérifié le 28/07/2016. [Consulté le 15/11/2016]. Disponible : https://www.service-public.fr/professionnels-entreprises/vosdroits/F32886

Lise Bernier. Polytechnique Montréal. [En ligne]. Publié le 21/07/2015. [Consulté le 14/11/2016]. Disponible : http://www.polymtl.ca/si/docs/documents/ORGANIGRAMME_SI_Juillet%202015.pdf

Yann Crispel. Cette copie de Windows n'est pas authentique. [En ligne]. Publié en août 2014. [Consulté le 20/11/2016]. Disponible : http://www.zebulon.fr/astuces/264-cette-copie-de-windows-n-est-pas-authentique.html

Adeo. Le droit de « Mastérisation » dans le cadre d'un parc de machines acquises via le canal OEM. [En ligne]. Publié le 15/01/2014. [Consulté le 20/11/2016]. Disponible : http://www.adeoinformatique.com/blog/2014/01/le-droit-de-masterisation-dans-le-cadre-dun-parc-de-machines-acquises-via-le-canal-oem/

Julien. Logiciels piratés : attention aux risques. [En ligne]. Publié en 21/11/2002. [Consulté le 20/11/2016]. Disponible : http://www.symantec.com/region/fr/resources/logiciel_pirates.html

Aline Hof. L'édito de MISC n°88 : Le mot de passe, ce grand cadavre à la renverse. [En ligne]. Publié le 31/10/2016. [Consulté le 10/11/2016]. Disponible : http://www.miscmag.com/?p=426

Dan Nguyen. 5 Ways Hackers are Stealing Passwords. [En ligne]. Publié le 12/03/2015. [Consulté le 20/11/2016]. Disponible : https://hypersecu.com/blog/91-5-ways-hackers-are-stealing-passwords

Le Monde. Piratage de Yahoo! : les réponses à vos questions. [En ligne]. Publié le 23/09/2016. [Consulté le 10/11/2016]. Disponible : http://www.lemonde.fr/pixels/article/2016/09/23/piratage-de-yahoo-les-reponses-a-vos-questions_5002273_4408996.html

Stéphane Calé, Philippe Touitou. La sécurité informatique. Paris: Lavoisier; 2007. p15-p17 & p118-p121.

OneLogin. One Time Password Solutions - OTP Authentication System - OTP Generator Software Service. [En ligne]. [Consulté le 20/11/2016]. Disponible : https://www.onelogin.com/product/one-time-password

ID Control. Biometric Authentication method Pro's and Con's - Keystroke Biometrics - Strong authentication with One Time Password, PKI and Keystroke Recognition. [En ligne]. [Consulté le 21/11/2016]. Disponible : http://www.idcontrol.com/keystroke-biometrics/biometric-authentication-method-pros-and-cons

NetMediaEurope. Guide pratique : Maîtriser l'automatisation des sauvegardes en 8 points - Livres blancs informatiques - Silicon.fr. [En ligne]. Publié en 2016. [Consulté le 20/11/2016]. Disponible : http://livreblanc.silicon.fr/resource/maitriser-lautomatisation-des-sauvegardes-en-8-points

Patrick. Sécuriser vos supports amovibles (clé usb, disque dur, carte mémoire, etc) | Le Blog de PEEXEL. [En ligne]. Publié en février 2016. [Consulté le 21/11/2016]. Disponible : http://www.leblogdepeexel.fr/securiser-vos-supports-amovibles-cle-usb-disque-dur-carte-memoire-etc/