Thème 1 Chapitre 2

Bloc 3 Cybersécurité des services informatiques

Compétence 3.1: Protéger des données à caractère personnel

SF3.1-4 : Sensibiliser les utilisateurs à la protection des données à caractère personnel

Mission 2

Sensibiliser les utilisateurs à la protection des données à caractère personnel

Mission

Les nombreuses irrégularités constatées imposent de mettre en place une campagne de sensibilisation sur la protection des données personnelles, à destination des opérateurs téléphoniques et de leurs managers.

Vous participez à l'élaboration et à la vérification des documents qui seront mobilisés pour cette campagne.

Travail à faire

1 - Précisez en quoi l'existence d'une charte informatique peut contraindre les utilisateurs du SI de CentreCall à être plus vigilants dans la protection des données à caractère personnel.

Documents 1 et 2

2 - Expliquez en quoi la publication de la charte informatique peut constituer un élément de sensibilisation des collaborateurs de CentreCall.

3 - Proposez d'autres supports de communication qui pourraient être réalisés dans le cadre de cette campagne de sensibilisation.

4 - Retrouvez comment CentreCall peut améliorer son fonctionnement grâce au RGPD

Document 3

Document 1

Extrait de projet de charte informatique

RÈGLES DE PROTECTION DES DONNÉES PERSONNELLES

1. Domaine d'application de la charte

Les règles décrites dans la présente charte s'appliquent à tout le personnel utilisant les moyens informatiques de CentreCall, ainsi que tout autre moyen de connexion à distance, afin d'accéder via Internet à tout service ou traitement électronique interne ou externe de l'entreprise, y compris l'accès à Internet.

Le non-respect d'une de ces règles est susceptible d'entrainer des mesures disciplinaires internes voire, en cas de violation d'un texte législatif ou règlementaire, des poursuites judiciaires. Les diverses lois concernant ce domaine sont présumées connues.

2. Conditions d'accès de l'utilisateur

- L'utilisation des ressources informatiques de l'entreprise est soumise à autorisation préalable.
- Cette autorisation est concrétisée par l'ouverture d'un compte utilisateur (création d'un courriel et d'un identifiant pour l'accès au réseau de l'entreprise).
- Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers.
- Cette autorisation ne vaut que pour les activités conformes aux missions de l'entreprise, dans le respect de la législation en vigueur.
- L'entreprise se réserve le droit de retirer à tout moment cette autorisation et ce, sans préavis.
- Chaque utilisateur doit user raisonnablement des ressources partagées auxquelles il accède.
- L'usage de ces ressources est, pour l'essentiel, dédié à des utilisations professionnelles.
- L'usage personnel doit rester limité.

3. Respect de la confidentialité des informations

- Les utilisateurs ne doivent pas tenter de lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.
- Les utilisateurs doivent s'interdire toute tentative d'interception de communications entre tiers.
- Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'entreprise.
- Les utilisateurs sont tenus de prendre, avec l'aide éventuelle du service informatique et du BPO (Data Protection Officer, délégué à la protection des données), les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par l'entreprise vis-à-vis de tiers.
- Une attention toute particulière doit être portée à la confidentialité des bases de données CentreCall. Leur utilisation doit respecter les engagements de CentreCall.

Document 2

Valeur de la charte informatique

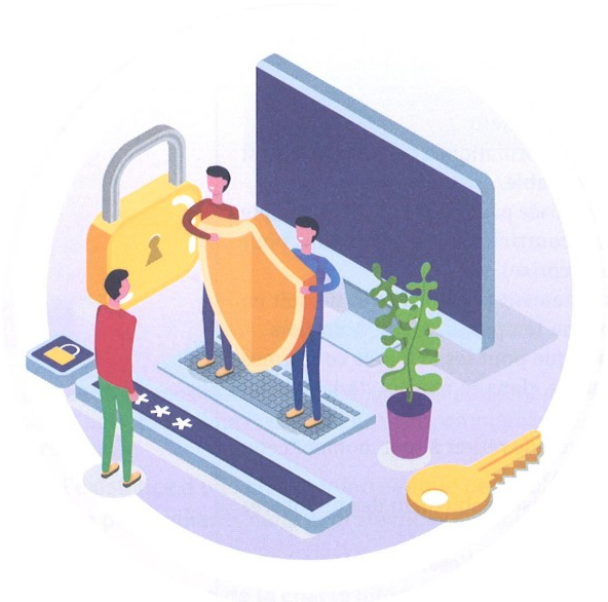
La charte informatique a la même valeur que le règlement intérieur si elle est adoptée en respectant les formalités et les règles de fond applicables par celui-ci (comme par exemple la consultation préalable des représentants du personnel).

Si elle est insérée au règlement intérieur, cela implique que celui-ci soit modifié en respectant les prescriptions du Code du travail.

Document 3

La législation sur la protection des données, une opportunité pour les entreprises

La législation sur la protection de la vie privée présente des exigences strictes et fait encourir de lourdes peines à ceux qui voudraient s'en affranchir ; elle est ainsi parfois perçue comme un fardeau, alors qu'il faut pourtant y voir là un véritable moteur, capable de dynamiser la croissance d'une organisation.



Optimiser les processus business

Les règles de confidentialité entraînent une plus grande transparence sur la collecte des données. Bien que les textes de loi ne les obligent pas tous à informer explicitement les clients de l'utilisation qui est faite de leurs informations personnelles, les entreprises doivent néanmoins procéder à un audit approfondi pour comprendre quel type de données elles stockent et pour quelle raison ; l'occasion aussi pour les organisations de se demander pourquoi elles collectent ces informations, si elles les exploitent efficacement et comment optimiser leur utilisation. Cette compréhension approfondie du flux de données offre une plus grande visibilité des **processus métiers**, et permet d'en tirer le meilleur parti.

Améliorer la gestion des données pour une meilleure rentabilité

Une fois qu'une entreprise a analysé l'ensemble de ses données, il est important qu'elle se pose la question suivante : « Ai-je besoin de tout ? » Et la réponse sera très probablement « non ». Ainsi, un contrôle continu dans un souci de conformité est un excellent moyen d'éliminer toutes les données superflues, telles que des fichiers redondants, obsolètes et inutiles, qui n'ont pas d'intérêt stratégique réel pour l'entreprise. En nettoyant les référentiels, il est également possible de réduire les coûts de traitement et de stockage des données, de mieux anticiper les éventuels frais si elles sont stockées dans le cloud et d'allouer le budget de façon plus pertinente. [...]

Réorganiser la stratégie de sécurité

Le coût lié aux failles de sécurité et au temps d'arrêt de l'activité d'une organisation suite à un vol de données critiques continue d'augmenter. Une raison supplémentaire, au-delà du respect de la législation, d'encourager les entreprises à revoir leur politique de sécurité. Il est en effet presque impossible de ne protéger que les données règlementaires et de laisser le reste de l'infrastructure informatique en dehors du périmètre surveillé.

Par conséquent, une organisation doit établir un contrôle strict de son activité dans l'intégralité de son environnement informatique, afin de mieux comprendre les risques qui s'y rapportent. À long terme, cela permettra d'investir davantage dans des ressources liées à la sécurité et de diminuer le risque d'incidents graves.

Pierre-Louis Lussan (country manager France, Netwrix!)

www.lesechos.fr, 17 juin 2019

1. Netwrix est un éditeur privé de logiciels de sécurité informatique.