DÉBAT À LA CFCIM

La sécurité de l'information, un enjeu majeur pour l'entreprise

La réunion d'information au sujet de «La sécurité de l'information», organisée le 12 février à la Chambre française de commerce et d'industrie du Maroc (CFCIM), fait partie d'un cycle dédié à l'importance de la formation, notamment sur les aspects numérique, juridique et financier relatifs à la gestion de l'information.

Au cours de la réunion animée par Karim Hamdaoui, expert en gestion des risques, sécurité de l'information, l'accent a été mis sur l'importance de la mise en place d'une stratégie au sein de l'organisation pour la gestion de l'information, garantissant la disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information. D'où l'importance de revoir ce concept en protégeant l'information et non le système de l'information uniquement, car la sécurité dépasse l'aspect technique et logistique des supports contenant l'information.

En effet, l'enjeu capital est tout d'abord humain, car l'être humain est également un support d'information. C'est en sensibilisant le personnel sur l'importance de l'information, qu'il devient possible d'assurer une protection étendue. Outre le facteur humain interviennent d'autres types de risques : de nature physique, par exemple (incendies, catastrophes naturelles...) pouvant nuire aux équipements contenant l'information. Ou bien de nature numérique, en minimisant le risque de fuite ou de contamination (externalisation des services, virus...).

Pour réussir à sécuriser les informations propres à l'entreprise, la mise à jour régulière s'impose que cela soit au niveau des mesures managériales, telles que l'encadrement et la formation, des mesures techniques, telles que l'installation d'antivirus, des mesures administratives, telles que l'intégration de clauses de confidentialité dans le contrat de travail ou des mesures juridiques, telles que la conformité aux lois et aux normes en vigueur à l'échelle nationale et internationale.

Le point avec Karim Hamdaoui, directeur général du cabinet LMPS Consulting.

Karim Hamdaoui
Directeur général du cabinet LMPS Consulting

Le Matin Emploi : Quels sont, selon vous, les enjeux inhérents à la sécurité de l'information ?

Karim Hamdaoui : Dans notre contexte actuel où les réseaux d'institutions de tout genre sont de plus en plus informatisés, interconnectés et ouverts sur l'extérieur, les enjeux liés à la sécurité de l'information sont nombreux et se présentent sous plusieurs formes. Les activités métiers et les stratégies au cœur même de la vie de l'entreprise s'appuient sur l'information produite, stockée et échangée par cette dernière. La perte, la modification ou le vol d'informations peuvent considérablement affaiblir une entreprise et remettre en question ses perspectives d'avenir.

De plus, en parallèle de l'évolution technologique que le monde connait ces dernières décennies, les menaces aussi bien externes qu'internes aux organismes ont elles aussi évoluées. Elles vont de pirates compétents, organisés et disposant d'outils aisément accessibles à l'insuffisance de sensibilisation des collaborateurs internes qui constituent le plus souvent le maillon faible de la sécurité de l'organisme.

Dans un tel contexte, l'information représente un actif aussi important que les actifs liés au système de production classique (actifs humains, sociaux, physiques, financiers...) et se doit d'être suffisamment protégée.

Qu'en est-il des process utilisés dans le domaine de la sécurité de l'information ?

Les processus de sécurité englobent la documentation, les moyens humains et matériels ainsi que les méthodologies et procédures visant à assurer la sécurité de l'information sur un aspect donné. Certains des plus importants sont les suivants :

- La gestion des risques : ce processus permet d'évaluer les risques pesant sur l'information, leurs impacts et de définir et mettre en œuvre les mesures de traitement appropriées.
- La classification et la manipulation de l'information : il s'agit de définir des mesures de protection appropriées au niveau de sensibilité de l'information.
- La sécurité physique et environnementale : Il s'agit de mettre en place des mesures préventives, de détection et de correction afin d'éviter des pertes de données dues à des catastrophes physiques.
- La gestion des actifs : les actifs informationnels et supports de l'organisme doivent être inventoriés, maîtrisés et placés sous la responsabilité de personnes formellement désignées afin de pouvoir en assurer une gestion et une protection adéquate.
- La gestion des accès physiques et logiques : le but est de préserver l'information des accès non autorisés et potentiellement préjudiciables.
- La gestion des modifications : permet d'éviter qu'un quelconque changement au sein de l'infrastructure ou des processus puisse occasionner des fuites ou pertes de données.
- La gestion des incidents : afin que les incidents de types sécurité soient traités dans des délais raisonnables de sorte à réduire l'impact ou même l'occurrence de ces derniers.
- La surveillance et la correction des vulnérabilités : cela passe par des audits techniques et organisationnels réguliers de la sécurité au sein de l'organisme.

Et quelles sont les difficultés liées à la mise en place de tels process ?

Les difficultés de mise en place des processus de sécurité varient d'un organisme à un autre selon la taille, l'organisation, les capacités financières et même la culture. Les contraintes les plus souvent rencontrées sont d'ordre :

- Stratégique : pour les organismes de grande taille et multi-sites, il n'est souvent pas aisé de définir le périmètre à inclure dans les processus de sécurité et d'obtenir l'adhésion de l'ensemble des parties prenantes.
- Organisationnel : les équipes internes de l'organisme manquent souvent de compétences pour assurer la mise en œuvre, le suivi et l'amélioration des processus de sécurité. Par ailleurs, l'organisation ne prévoit parfois pas un pilote désigné et dédié au projet de sécurité.
- Structurel : les organismes possèdent le plus souvent une structure et des processus en vigueur où doivent s'intégrer les processus de sécurité. Cette intégration génère parfois des conflits entre personnes ou entre processus.
- Budgétaire : les coûts de mise en place se révèlent souvent assez élevés selon le modèle d'accompagnement choisi, la taille ou l'infrastructure de l'entreprise. Ces coûts augmentent considérablement lorsqu'il est question de se certifier par la suite.
- Culturel : certaines cultures, par exemple, ne voient en les normes de sécurité qu'une «façade» exigeant beaucoup de documentation pour peu de concret et d'autres perçoivent les mesures et exigences de sécurité comme génératrices de charge de travail supplémentaire.

> «Les processus de sécurité englobent la documentation, les moyens humains et matériels ainsi que les procédures visant à assurer la sécurité de l'information.»

D'après vous, quel est le rôle de la direction des ressources humaines dans la participation à la protection de l'information ?

Dans la démarche de sécurité de l'information, la Direction des ressources humaines joue un rôle important. Elle est garante de mesures préventives et dissuasives, en ce qui concerne surtout les menaces internes. Du recrutement au départ ou mutations des collaborateurs, elle doit assurer un suivi minutieux afin que les mouvements au sein du personnel n'entravent pas la sécurité de l'information. La Direction des ressources humaines doit donc s'assurer que les nouveaux collaborateurs sont assez fiables et adhèrent à la culture de sécurité en place ; cela à travers la sensibilisation, la formation de ces derniers et si nécessaire, l'application de mesures disciplinaires. Quant aux collaborateurs en fin de contrat, elle doit s'assurer qu'ils ne conservent pas des actifs ou des accès aux actifs de l'organisme et que des secrets professionnels ne soient pas divulgués. «

Propos recueillis par M.S.

Le Matin du 17/02/2014