SECURITE INFORMATIQUE : AVEC QUELS MOYENS ?

Vélizy, le 2 septembre 2015

LA CYBERSECURITE A THALES

Il y a quelques semaines, THALES se faisait épingler par un article du Canard Enchainé. On y apprend qu'en décembre dernier, l'ensemble des postes serveurs et équipements « Etatsunien » a été infecté. On y apprend également que dans le cadre du programme SIC21 (fourniture de systèmes informatiques à la Marine Nationale), nous aurions livré du matériel potentiellement vérolé par le virus Crouch Yeti.

UN MANQUE CRUCIAL DE MOYENS

Suite à ces attaques, la DSI (Direction des Systèmes d'Information) a mis en place un programme de sécurisation avec notamment une campagne de réinitialisation des mots de passe. Problème : celle-ci a été lancée courant mai, période où presque tout le monde pose ses reliquats de congés. Alors à la rentrée, devant l'afflux des requêtes, les pauvres serveurs de messagerie, qui méritaient bien d'aller à la retraite, n'ont pas supporté… 24h00 de paralysie de notre société, tout cela pour avoir mégotté sur le changement de matériel notoirement obsolète !

Certes, ce n'est pas facile de faire face à ce que l'on peut maintenant appeler une guerre et nous sommes conscients que toutes nos équipes mettent tout en œuvre pour nous protéger. Mais cela demande des moyens matériels et humains à la mesure qui, aux yeux des financiers, ne sont pas compatibles avec tous ces plans d'économie, au dépend « on le voit ici » de notre sécurité. Ce n'est pas compatible non plus avec une politique de sous-traitance à tout va, qui, heureusement est de plus en plus décriée.

SECURISER LES EMPLOIS POUR LA SECURITE INFORMATIQUE

Pour se protéger de cette cyber-guerre, le Groupe doit se donner les moyens nécessaires : moyens humains et moyens matériels.

Les moyens humains doivent être qualifiés, convenablement formés, et exerçant leur activité dans des conditions de travail permettant une efficacité sereine, et déployés au plus près des sites et des collègues utilisateurs.

Pour bien faire, les moyens matériels devraient être indépendants des grands fournisseurs US ou Chinois, et le Groupe doit donc se poser la question de la ré-internalisation des composants critiques « cœurs de sécurité », au moins au niveau européen (se rapprocher par exemple de ST Microélectronics et des fondeurs indépendants). Cette politique doit être en cohérence avec les contraintes de la cybersécurisation des systèmes et composants, qui passent par une plus grande maîtrise du Hardware, et de la localisation physique des données (Data centers privés et contrôlés). Se pose également la question du développement d'un middleware[1] spécifique, dédié aux applications sensibles du Groupe, indépendant des Google, Windows, Amazone et autres …

[1] un middleware ou intergiciel est un logiciel tiers qui crée un réseau d'échange d'informations entre différentes applications informatiques.

LANCEUR D'ALERTE !

Dans une de nos filiales, les militants CGT ont interpellé, en CCE, un directeur des systèmes d'information en posant les questions suivantes :

- Suite au choix politique du Groupe d'externaliser le service informatique de proximité, quelles en sont les conséquences opérationnelles et les problèmes rencontrés ?
- Comment mener à bien les objectifs du service de proximité et répondre aux besoins des salariés en termes de service ?

Voici les réponses faites par ce directeur (extrait du PV) :

« Nous avons alerté sur le service de proximité, de manière générale, sur les sites Thales, dans La mesure où nous voyons les effectifs diminuer. Le phénomène de diminution générale des services de proximité est dû au fait que le Groupe a automatisé et automatisera encore plus, notamment la fabrication des postes …».

« Nous sommes vigilants et nous demandons de ne pas commencer à compresser les équipes, alors que nous sommes au milieu du gué et que les choses ne sont pas totalement automatisées. Le dialogue avec le Groupe n'est pas aisé. On ne remplace pas un service par un autre tant que le nouveau service n'est pas opérationnel. Tel est le débat actuel avec le Groupe et nous en souffrons beaucoup ».

« Nous cherchons à convaincre le Groupe de conserver un minimum de compétences Thales, ne serait-ce que pour des questions de sécurité, tous les prestataires n'ayant pas accès à tout, il y a un équilibre à trouver. Faire appel à des compétences externes ne nous permet pas de capitaliser et pour l'avoir vécu sur un certain nombre de projets depuis plusieurs années, je sais qu'il faut une proximité forte avec le business, avec nos sites »

QUELLES CONSEQUENCES ?

Il découle de ces choix politiques une détérioration des conditions de travail, un mal-vivre et un mal-être amplifiés par des objectifs peu tenables en terme de moyens et avec une pression permanente sur le personnel concerné.

Le management par des critères quantifiés et des objectifs chiffrés, chronométrés, en évaluant des salariés par des statistiques, par un contrôle permanent et par des demandes de justifications incessantes conduit forcément à une mauvaise qualité de vie au travail des salariés.

QUEL POSITIONNEMENT AU NIVEAU GROUPE ?

Tous ces sujets deviennent des priorités et demandent des réponses appropriées. Cela devient une urgence. N'oublions pas que notre Groupe a comme prétention d'être un leader mondial des produits et solutions de sécurité. Gardons cette reconnaissance en matière d'intégration des systèmes complexes et de grandes envergures.

Mais peut-on relever le défi de la cybersécurité avec les moyens actuels ?

Nous pensons que tous ces enjeux, qui touchent la sécurité nationale, la sécurité urbaine, les infrastructures critiques, le cyberespace, doivent avoir des moyens à la hauteur des enjeux.

Il est temps d'investir, de donner de véritables moyens aux équipes, avec un renforcement en emploi pérenne et stable, de privilégier la qualité du service et de l'écoute tout en permettant aux salariés de bien travailler et ceci dans de bonnes conditions.