Un souci dans l'énoncé ? – La Mare du Gof

Il y a quelques jours, je « twittais » ceci avec une certaine malice (cf. ci-dessous). L'actualité PRISM, en écho aux accents français cyber guerriers de tous les colloques de ces derniers mois, avec un zeste de déclarations publiques d'appel au « cloud souverain », cumulés avec une expérience en pratique au sein d'une institution, et mes souvenirs de l'article de Manach… Tous ces éléments me font dire qu'il y a foutage de canard.

Il y a quelques temps, j'ai eu l'occasion de voir comment cela se passait dans une administration « ordinaire » dans ses relations électroniques avec des prestataires extérieurs. Il s'agissait ici d'un service de communication, appelé donc à transmettre des pièces-jointes volumineuses (ou à en recevoir) auprès de leurs prestataires (imprimeurs, entités subordonnées ou hiérarchiques délocalisées, infographistes ou publicitaires extérieurs, etc.). Les fonctionnaires n'ont la main sur aucun élément de configuration de leurs réseaux, messageries et espaces de stockage, systèmes et environnement, le tout étant maitrisé par une entité distante dédiée, suivant, je l'imagine, les strictes règles édictées de l'ANSSI. Ainsi, faute de pouvoir converser et échanger des pièces avec leurs prestataires, ou en raison de la taille trop volumineuse des pièces ou de la nature des fichiers qui ne passent pas par les filtres édictés, les agents se sont créés des adresses mail semi-professionnelles sur des plateformes webmail à caractère privé (gmail, yahoo, hotmail, etc.). Les pièces sont ainsi stockées en ligne, qui via google, skydrive, amazon, dropbox sur une machine internet, utilisent des services de transferts de fichiers (type « wetransfer.com » ou autres) et communiquent à leurs contacts extérieurs leurs adresses semi-professionnelles. Il va sans dire que le transfert des pièces des machines isolées (intranet) aux machines connectées à la Matrice se passe au mieux par messagerie –professionnelle vers semi-professionnelle (lorsque c'est uniquement le format des fichiers qui bloquaient les transferts), au pire par clé USB –personnelle- d'un poste à l'autre lorsque c'était le volume des données qui engendrait le blocage, avec la réciprocité des transferts que cela sous-entend.

D'une part, on connait la vulnérabilité de nombreuses plateformes webmail, surtout due à l'insuffisance de précaution de leurs utilisateurs (question secrète, double authentification, réinitialisation des mots de passe, etc.), parfois due à la configuration technique de la plateforme même du service. On connait également l'absence de confidentialité de ces plateformes, par des agents privés dans un cadre Marketing et publicitaire, ou des agents institutionnels, PRISM nous le rappelle encore pour ceux qui s'obstinaient à en douter. A ce propos, il est amusant de noter qu'il y a plusieurs années, à l'énoncé de cette réalité d'absence de confidentialité nos « experts » criaient *halte à la théorie du complot et des paranos*. A présent qu'un Snowden a donné quelques documents, ces mêmes « experts » nous disent que c'était su de tous et qu'il n'y a là rien de nouveau, tandis que la presse et certains politiques redécouvrent l' « ordre des choses » alors que c'était clamé par beaucoup depuis tant d'années. Que d'énergie gâchée à contredire une réalité au lieu de s'y adapter et de former les personnels…

D'autre part, l'immense majorité des systèmes de nos administrations et institutions étant du Windows (l'actualité du « Pack Open Bar Microsoft » dans la Défense est encore fraiche à nos oreilles et on attend toujours les réponses aux questions de l'Assemblée Nationale), les mises à jour étant centralisées chez de supers administrateurs délocalisés, l'absence criante de celles essentielles (systèmes Windows, patch correctifs d'applications tierces) est manifeste. J'imagine que les correctifs n'ayant pas été audités, ils ne sont pas appliqués, l'urgence étant moindre du fait supposé d'absence de porosité entre ces réseaux « intra » et la Matrice. Rien n'est moins faux finalement. Par-dessus, de nombreux outils de publication (CMS) de diverses plateformes institutionnelles à vocation de communication à destination du grand public sont indiscrets par défaut, voire vulnérable via l'implémentation de technologies tierces non maitrisées. Enfin, les utilisateurs sur les machines institutionnelles ne peuvent –pour ceux sensibilisés- envisager de technologies de chiffrement autres que celles supportées par les administrateurs et allouées qu'au compte-goutte aux seuls individus dont la fonction exige un chiffrement des données. Que dire de simples applications Windows comme un KeyPass interdites sur les postes au prétexte qu'elles ne sont pas dans le « catalogue » induisant de fait une simplification des trop nombreux mots de passe à générer et retenir pour le fonctionnaire. Qui a déjà vu un fonctionnaire non spécialisé échanger une clé PGP professionnelle ?

Monsieur Pailloux recommandait il y a peu de revenir aux fondamentaux, aux règles de bonne hygiène informatique. Il y a pourtant manifestement une dichotomie entre ce qu'il leur est possible de faire et ce qu'il leur est demandé de faire, quel que soit le ministère. Les utilisateurs s'adaptent comme ils peuvent à l'objectif assigné, introduisant de fait des vulnérabilités. Nul doute ici que plutôt d'envisager de corriger les CMS indiscrets, d'auditer par les services spécialisés les insertions d'entreprises tierces sur ces mêmes CMS ou les éventuelles applications open source utiles au tout venant,

d'allouer des espaces de stockage à la dimension des objectifs assignés aux missions des uns et des autres, et d'affiner les règles de messagerie, le bridage des fonctionnalités disponibles sera encore plus important- induisant une adaptation encore plus dangereuse des agents- au nom de l'économie de moyens.

« *Alors que le Pentagone se prépare sérieusement à la "cyber-guerre", tout comme la gendarmerie française, il est frappant de constater des failles béantes dans la sécurité des administrations nationales. Le gouvernement dépense des dizaines de millier d'euros pour assurer la sécurité de ses communications privées (voir chez Thales, par exemple). L'utilité de ces défenses est sérieusement diminuée si un assaillant peut avoir accès à de nombreuses boîtes e-mails au sein de l'administration* », 2010 Jean-March Manach. Combien aujourd'hui ? Une simple recherche via les moteurs grands publics retourne une quantité impressionnante de résultats. J.M. Manach n'évoquait dans son article que les accès frauduleux, par filouterie essentiellement d'individualités. Il n'abordait pas dans son article le cas basique de l'intelligence économique entre états (qu'est PRISM sous couvert de lutte antiterroriste ?).

Bref, on marche sur la tête et il y a du taf. Le canard a quelques pigeons à élever et vous suggère d'en faire autant… Je me doute qu'il y a des choses qui m'échappent, et que l'exemple vécu ne saurait avoir valeur de généralités. Pour autant, les bonnes pratiques ne commencent-elles pas par l'ajustement des moyens techniques aux objectifs assignés, plutôt qu'à hypocritement les ignorer ? Ou alors ne faut-il pas revoir à la baisse les objectifs ?

Crédit photo FlickR Orwellian eye de Gaellery sous CC.

Lien du billet en ligne.