Syndicats CGT et SUD de l'Insee
Déclaration liminaire sur le RSSI pour le CTR du 23 janvier 2014

L'examen du rapport sur la sécurité des systèmes d'information est toujours délicat puisque nous devons analyser un rapport sur l'activité de l'année passée dans un domaine où la course entre sécurisation et « crackage » des protections est une course de vitesse permanente…

Mais comme il s'agit aujourd'hui de la première fois où nous pouvons traiter le point sécurité des systèmes d'information en comité technique, nous traiterons également de sujets plus structurels.

Notamment, nous estimons que la question de la sécurité des systèmes d'information n'est pas prise en charge et coordonnée à la mesure de ce qu'elle devrait être au sein de notre institut. Cela ne veut aucunement dire que nous estimons que la direction ainsi que l'ensemble des agents ne sont pas préoccupés par cette question. Cela signifie que la coordination et l'implication de la direction de l'Insee sur la sécurité des systèmes d'information ne transparaissent que très peu, même au travers du rapport qui est leur est dédié.

En effet, bien que désormais mieux structuré et plus précis, la lecture du rapport montre peu de choses : la sécurité des données est partiellement traitée, celle des bâtiments, pourtant indissociable de la question de la sécurité des données est inexistante.

Il y manque également une vision globale de la sécurité à l'Insee. L'environnement général, interministériel, est présenté sans qu'on puisse lire comment l'Insee se situe en son sein. Très souvent, nous sommes amenés à nous dire : « Oui, et alors ? » ou « Qu'en est-il à l'Insee ? ». Des audits ont été réalisés : soit, mais qu'en est-il ressorti ? pour l'établissement ou l'application concernés ? Pour les autres établissements et les futures applications ?
Il manque une vision politique cohérente à mener par la direction de l'Insee, que ce soit au niveau national ou local.

- ✓ **Sur la sécurité physique des bâtiments :**

La sécurité des bâtiments n'est absolument pas abordée dans ce document, alors que c'est une préoccupation de plus en plus prégnante avec la banalisation du partage des locaux avec d'autres organismes. Or la sécurité des systèmes informatiques peut être très performante mais complètement annihilée par des défaillances d'organisation. Pour nous la sécurité des systèmes d'information est donc bien un tout qu'il faut traiter de manière coordonnée.

Les conseillers locaux de sécurité (CLS) étant généralement recrutés sur leur connaissance d'un domaine en particulier, nous proposons aujourd'hui d'engager une réflexion sur l'opportunité d'un binôme de CLS, un-e plus sur les questions informatiques, l'autre plus sur les questions de locaux.

La sécurité des données et des bâtiments ne doit pas être traitée à minima c'est pourquoi la direction de l'Insee doit réinvestir ce domaine, sans tomber dans le sécuritarisme et en veillant à ce que les mesures mises en place n'empêchent pas les agents de mener à bien leurs travaux.

Notamment, il y a un réel besoin de mettre au point des procédures de sécurité efficaces, pratiques, et correctement diffusées : très souvent les procédures, trop complexes et mal documentées, ne sont tout simplement pas applicables par toutes et tous dans le quotidien du travail. Sur le terrain, les personnes chargées de mettre en œuvre le partage des locaux (logistique, informatique,...) devraient avoir un mémento des actions à mettre en œuvre, celles proscrites, etc. Ce mémento pourrait être enrichi des différentes expériences ayant eu lieu dans les établissements.

- ✓ **Sur la politique de formations des agents et la communication :**

Depuis plusieurs années, nous avons régulièrement demandé la mise en place d'actions de sensibilisation et de formation régulières sur la sécurité des systèmes d'information à destination de l'ensemble des agents. Nous renouvelons aujourd'hui cette demande devant déboucher sur une mise en œuvre rapide. Un petit guide sur la sécurité des données à l'Insee serait une marque de la prise en compte de notre demande. Les éléments liés à cette sécurité devraient être présentés lors de l'arrivée d'un nouvel agent dans un établissement.

- ✓ **Sur les questions de sécurité « internet » :**

En 2013, les attaques contre les sites internet (pages web, applications web et base de données,...) se multiplient : en plus du site statistique-publique.fr, citons récemment France Télévisions, la base de données des urgences des hôpitaux, la CNIL et même l'ANSSI. Compte tenu des orientations de l'Insee de mise en ligne des questionnaires d'enquêtes (homère, capi3G, hôtellerie, enquêtes entreprises,...), cela ne peut aller qu'avec un dispositif de surveillance et d'alertes de haut niveau.
Nous demandons des explications sur l'allègement de la sécurité des mots de passe page 5 du rapport.
Enfin, certains accès à des sites internet sont nécessaires au travail des agents : leur blocage simple n'est pas une solution ! Si une bonne communication était réalisée, chaque agent saurait qu'il est possible de demander à faire débloquer un site.

- ✓ **Sur la sécurité des équipements informatiques :**

Nous demandons qu'une analyse sur l'usure des matériels soient faites. Si les unités centrales bénéficient d'un bon renouvellement avec le passage à windows 7, les serveurs des DR commencent à dater. Nous attirons donc votre attention sur ces matériels vieillissants, trop faibles en capacité de stockage mais qui contiennent les données de travail de milliers d'agents.

Enfin, il nous semble grand temps que l'Insee s'intéresse aux nouveaux matériels utilisés par les agents. Après les clés USB, le quotidien est fait de disques durs externes, lecteurs MP3, tablettes, smartphones qui ont des usages multiples avant et après être branchés sur des ordinateurs de l'institut. Nous ne souhaitons pas le développement de mesures sécuritaires. Par contre, nous souhaitons qu'un guide de bonnes pratiques soit réalisé et diffusé.

- ✓ **Sur la sécurité des logiciels :**

Le passage de windows Xp à windows 7 s'inscrit dans la nécessaire mise à niveau d'un point de vue sécurité. Les conditions de déploiement sont révélatrices des orientations de l'Institut : manque de personnel pour mettre à disposition le système qui a pris plusieurs mois de retard, manque d'effectifs dans les Ressources Informatiques locales pour déployer le système. Si les agents se voient proposer une auto-formation tutorée, aucun dispositif de formation national pour les informaticiens n'est prévu. Certains établissements auront les moyens de former leurs informaticiens, d'autres non. Et ce n'est pas l'assistance à distance qui permettra aux informaticiens de proximité de rendre les services aux utilisateurs. D'ailleurs les directions régionales elles-mêmes demandent une pause dans la baisse des effectifs.

Les logiciels s'appuyant sur les technologies Java ont subi plus de 14 millions d'attaques entre l'été 2012 et l'été 2013. La politique de mise à jour d'Oracle (qui gère Java) n'est pas assez énergique. Nous souhaitons qu'une veille particulière soit faite avec CAPI 3G qui sera développé en java et ouvert sur internet pour un nouveau type de collecte.

En 2013, 99% des attaques malveillantes mobiles ont ciblé androïd, système équipant les smartphones de l'Insee. Il est pour nous grand temps qu'une politique de sécurité, figurant dans le rapport annuel SSI, soit mise en œuvre. Il est pour nous incohérent de laisser des matériels non sécurisés de l'Institut

accéder à internet et à la messagerie alors que les postes en XP seront coupés du monde extérieur à partir du 8 avril.

La société McAfee (l'anti-virus utilisé à l'Insee) va disparaître après son rachat par Intel. La disparation et le remplacement par un autre antivirus est prévu d'ici un an, Une étude du RSSI Insee serait utile pour décider s'il faut continuer avec « un programme de scan de virus à peine passable qui tend à rendre l'ordinateur complètement inutilisable lorsqu'il démarre une mise à jour », d'après son créateur...

- ✓ **Sur la disponibilité du réseau et les postes nomades :**

Nous vous demandons des réponses sur les dysfonctionnements des postes nomades des enquêtrices et enquêteurs : qu'allez vous faire pour nos collègues qui sont en zone blanche des opérateurs téléphoniques : où en êtes vous de l'achat de clés 3G auprès d'autres fournisseurs d'accès ?

Aucun agent de bureau ne supporterait d'allumer son PC le matin et ne pas pouvoir se connecter au réseau. Or c'est ce qui passe pour certaines de nos collègues sur le terrain, les obligeant ainsi à faire des kilomètres pour trouver un lieu couvert par le réseau SFR.

D'autre part, si nous pouvons comprendre la sécurité mise en place sur leurs postes nomades, les dysfonctionnements dégradent fortement leurs conditions de travail : non information sur l'expiration du mot de passe, non accès au serveur CAPI si le poste n'est pas à jour alors qu'il était prévu que le téléchargement et la transmission des questionnaires soit toujours possible,...

Nous savons ce sujet ingrat : une faille découverte, et toutes les autres protections pourtant mises en œuvre semblent dérisoires. C'est pourquoi nous souhaitons entendre votre engagement à coordonner une politique ambitieuse sur la sécurité des données que nous avons pour mission de traiter.

Nous attendons donc vos réponses et des engagements sur les motions que nous proposons.