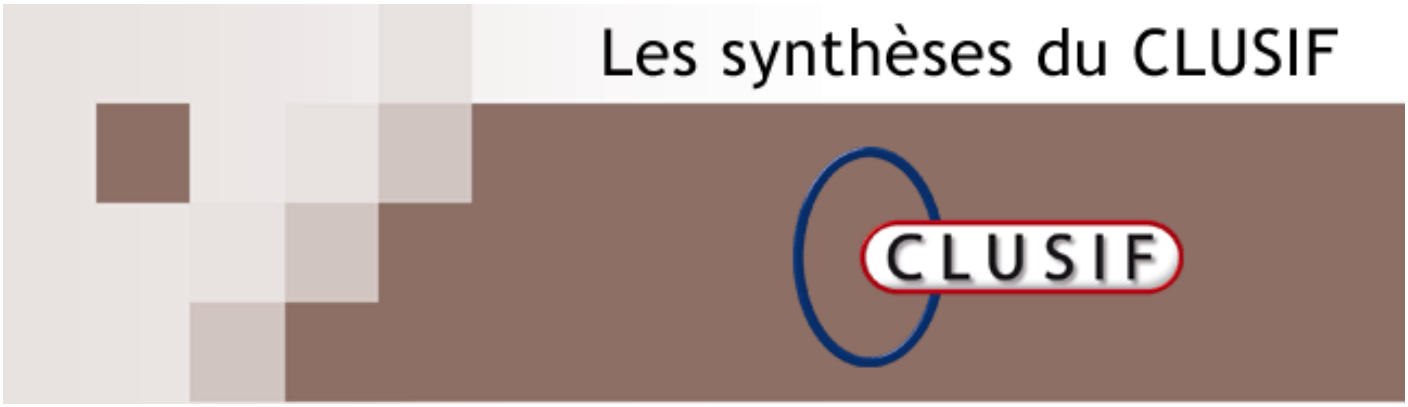

La Sensibilisation : pour qui, pourquoi et comment - *Synthèse de la conférence thématique du CLUSIF du 17 juin 2015.*

Il est courant d'entendre que « *Le problème dans l'informatique c'est ce qui est entre l'ordinateur et le fauteuil (i.e. l'utilisateur)* », mais la vérité est que si, en tant que partie intégrante du système d'information, l'humain est en effet porteur de risque, il est avant tout un formidable vecteur de progrès.

Pour autant, la considération du facteur humain dans la SSI par les DSI[1] n'est que de 13%[2]. Mais alors, quel gain une entreprise peut-elle attendre de la simple éducation de ses utilisateurs à la SSI ? Cette sensibilisation ne devrait-elle pas être élargie au-delà de l'entreprise pour s'adresser à la société civile et être délivrée aux jeunes générations ?

Pour apporter des éléments de réponse à ces problématiques, les personnalités suivantes sont intervenues : Bruno SIDO (Sénateur, premier vice-président de l'OPECST[3]), Jean-François PEPIN (CIGREF), Damian NOLAN (DAesign), Antoine BAJOLET (TDF), Fabrice NERACOULIS (SNCF), Lazaro PEJSACHOWICZ (CNAMTS), Jean-Eudes LHERBIER (CPAM de la Marne) et, animateur de la table ronde, Jean-Marc GREMY (Cabestan Consultants).

Quelle doit être la cible de la sensibilisation ?

Dans le cadre d'une entreprise, la sensibilisation doit affecter l'ensemble des utilisateurs du système d'information. Pour cela, il est nécessaire d'impliquer très tôt la Direction pour ensuite s'adresser aux collaborateurs. Commencer par la Direction permet d'obtenir de cette dernière les moyens (financier, temporel, humain, …) nécessaires pour mener à bien cette sensibilisation, mais aussi de s'adresser à la catégorie de personnes susceptibles de manipuler les informations les plus sensibles pour l'entreprise. Pour autant cette sensibilisation peut (doit ?) être abordée hors du cadre de l'entreprise et élargie à l'échelle de la société. En effet, la sensibilisation sur la SSI doit intervenir auprès de la jeune génération[4], dite « du numérique », afin de faire prendre conscience aux citoyens des bénéfices et des dangers du numérique.

Quelle doit être la forme du message de sensibilisation ?

L'importance d'une sensibilisation réussie réside en plusieurs principes. Premièrement, le message que l'on souhaite faire passer doit être le plus clair et le plus concis possible afin de ne pas noyer la cible dans du contenu superflu et ainsi risquer de la perdre. De plus, le message ne doit pas être anodin, il doit être en lien avec un événement qui a touché la cible afin que la sensibilisation soit plus efficace (spam, phishing, …). Ensuite, le message doit être impersonnel et non pointer nominativement les mauvaises pratiques au sein de l'organisation. Le rappel aux sanctions encourues en cas de non-respect des bonnes pratiques énoncées est à bannir de tout support de sensibilisation. Enfin, la sensibilisation et le support associé doivent être un refuge pour l'utilisateur faisant face à une situation qu'il ne contrôle pas. Ils doivent donc, notamment, indiquer un point de contact pour que l'utilisateur

[1] Direction des Systèmes d'Information

[2] Fabrice NERACOULIS, « Retour d'expérience SNCF : quel plan de sensibilisation pour quels résultats »

[3] http://www.assemblee-nationale.fr/commissions/opecst-index.asp

[4] Bruno SIDO, « La sensibilisation au cœur des préoccupations nationales »

puisse poser ses questions ou remonter toute incohérence entre les mesures de sécurité mise en œuvre et les pratiques opérationnelles dans l'entreprise[5].

Quel doit être le moyen de diffusion du message de sensibilisation ?

Le moyen de diffusion du message doit être le moins rébarbatif possible. Pour cela, le cours magistral sur la SSI, longtemps adopté dans les entreprises pour sensibiliser les collaborateurs, tend à disparaître. Peu interactif, aucun changement notoire n'a été constaté dans le comportement des collaborateurs[6] à la suite de ces sessions. Ainsi, la sensibilisation a pris de nouvelles formes et couleurs pour s'appuyer sur des références connues (BD, …) ou sur des personnages, créés par le service de communication et portés à l'attention des utilisateurs par des supports mis à disposition sur l'intranet ou par des « goodies ».

Puis, depuis quelques années, on observe l'émergence d'un nouveau type de sensibilisation, les « *Serious Game* »[7], ou jeux interactifs, dans lesquels le joueur, en l'occurrence un collaborateur, est mis dans une situation réaliste représentant un risque pour la SSI (domicile, gare, train, entreprise) et va devoir, par le biais d'actions réflexes ou au contraire réfléchies, prendre des décisions. L'utilisateur peut ainsi acquérir les bonnes pratiques de lui-même en apprenant de ses erreurs.

[5] *Lazaro PEJSACHOWICZ, Jean-Eudes LHERBIER, «* Retour d'expérience CNAMTS : déploiement différencié à grande échelle »

[6] Antoine BAJOLET, Damian NOLAN et Jean-François PEPIN, « Un *Serious Game* au service de la sensibilisation : finalités, moyens et premiers retours »

[7] Damian NOLAN, DAesign, éditeur du « Serious Games » *Keep An Eye Out*