



CSO Interchange – Paris 2008

Tendances 2008 : des menaces toujours très présentes, mais l'humain de plus en plus au cœur des préoccupations des RSSI

Paris, le 27 Juin 2008 – Organisé pour permettre aux RSSI, DSI et autres responsables de la sécurité informatique dans les entreprises d'échanger leurs expériences et bonnes pratiques, le CSO Interchange 2008 a mis en lumière leurs préoccupations en matière de sécurité informatique. Cette année encore, les menaces internes apparaissent comme un élément majeur à surveiller en matière de sécurité de l'entreprise, ainsi que la déperimétrisation du réseau qui reste un sujet critique pour la DSI. C'est, en effet, ce que révèlent à la fois, les résultats du questionnaire posé durant la journée et les conclusions des tables rondes proposées.

« Le métier de RSSI a largement évolué ces dernières années, au même titre que le marché de la sécurité informatique. Aujourd'hui, nous ne pouvons plus nous limiter aux informations fournies par les éditeurs ; nous avons besoin d'autres sources et, qui mieux que les RSSI peuvent nous fournir un retour d'expérience pertinent et objectif ? », déclare **Didier Gras**, Senior Manager de l'activité TMS (Threat Management Services) d'Alcatel-Lucent/BU Security Practice. « Etre réunis tout au long d'une journée et échanger autour de problématiques directement liées aux préoccupations sécurité des entreprises est particulièrement enrichissant pour la population des RSSI. Un événement comme CSO Interchange est un rendez-vous qui mérite donc toute attention. »

2007-2008, les mêmes préoccupations mais des missions toujours plus complexes

Questionnés sur leur environnement et la sécurisation de leur réseau d'entreprise, plus de 70% des RSSI présents ont déclaré craindre les menaces internes, un chiffre similaire à celui de l'an dernier, mais surtout quasi identique à celui obtenu lors du CSO Interchange de Londres. Et ce sont les employés qui gardent la première place dans la liste des risques recensés !

Quant à la sécurisation du réseau informatique et la mise en conformité, cela reste toujours plus ardu pour plus de 50%, et à l'identique pour 33% des participants (chiffres proches de ceux collectés en Angleterre pour la même question). De plus, l'essor de nouvelles technologies, tels que les réseaux sociaux, le WEB 2.0... mais également, l'augmentation des réglementations auxquelles les entreprises sont de plus en plus assujetties, sont autant de facteurs qui participent à la complexité des missions des RSSI.

Des RSSI qui, malgré l'évolution des demandes et des priorités de l'entreprise, n'ont pas été nommés pour autant à des postes de Risk Manager et/ou de contrôleur interne informatique (seuls 40% d'entre eux ont vu leur profil de poste être modifié). En effet, dans une forte majorité des cas, ce sont les Directions Générales ou Directions Financières qui se chargent de ce poste (respectivement 57,6% et 9,1%), ils sont seulement 15% à revendiquer cette mission. Un autre élément participe aux difficultés que rencontrent les RSSI : le budget qui est un frein majeur pour la réalisation de projets de sécurité (55%), suivi par le manque de temps et de technologies à place égale avec le manque de ressources humaines. Des résultats presque similaires avec l'Angleterre, même si les RSSI britanniques positionnent le manque de temps et de ressources avant les freins budgétaires (l'insuffisance des technologies n'arrive qu'en 4^{ème} position).

Enfin, la mise en conformité est pour 23% des répondants, l'un des principaux facteurs de motivation pour la mise en place d'une politique de sécurité. On peut même dire que la sécurité s'améliore grâce à la mise en conformité, qui apporte de la valeur à l'entreprise. Cependant, les réglementations et les normes sont, tous les ans, de plus en plus nombreuses.

Les nouveaux usages influencent de plus en plus les politiques informatiques

Concernant le périmètre de l'entreprise, tous s'accordent à dire que depuis quelques années, l'entreprise s'est totalement « déperimétrée ». Réseaux sociaux, évolution grandissante des outils informatiques mobiles, accroissement de la productivité... sont les principaux facteurs qui poussent aujourd'hui les entreprises à repenser leur politique de sécurité. Ainsi, l'utilisation des nouveaux outils liés au web 2.0 est considérée, par plus de 70% des RSSI présents, comme une menace. En effet, la volonté des entreprises à favoriser la production des collaborateurs en leur laissant la liberté d'utiliser leurs outils informatiques en dehors de l'entreprise, et surtout l'essor de services tels que les instant messenger et autres... laisse une porte grande ouverte aux attaques.

Ainsi, de nombreux RSSI présents ont mentionné, lors des tables rondes qui ont ponctué la journée, la nécessité de communiquer et de sensibiliser les collaborateurs de l'entreprise aux enjeux liés à la sécurité informatique et à la protection des données de l'entreprise.

« Les résultats collectés cette année viennent conforter nos points de vue chez IDC. Les entreprises rencontrent souvent les mêmes problèmes, qu'elles soient françaises, américaines ou anglaises. Elles sont soumises à des réglementations internationales, aux mêmes utilisations du web 2.0... mondialisation oblige ! Les réponses de confiance pour les aider à gérer finement ces problématiques se font un peu attendre. Il y a bien du bruit marketing autour de certaines solutions mais les besoins sont complexes à adresser. Assez étonnement, beaucoup de solutions sont déjà en place pour couvrir les besoins très étroits de contrôle de l'information (DLP), mais il manque encore une réponse globale », constate **Eric Damage**, Directeur de Recherche Europe, IDC. « La rencontre entre professionnels telle que CSO Interchange le permet, est un moment riche pour les RSSI. Ils peuvent y partager beaucoup d'expériences, entendre des témoignages avancés et bâtir leur réflexion sur un retour d'expériences concret, réaliste et sans langue de bois. »

Une prochaine édition du CSO Interchange sera programmée au 1er semestre 2009 et sera ouverte à tous les RSSI souhaitant partager et faire partager leur expérience.

A propos de CSO Interchange

CSO Interchange est un forum d'échanges non mercantile et sans aucune présence commerciale, réunissant pendant une journée, des Responsables de la Sécurité Informatique pour leur permettre de discuter des dernières tendances du secteur, d'échanger des idées et de débattre des problématiques émergentes auxquelles ils sont confrontés.

CSO Interchange est une organisation non lucrative et non commerciale, fondée par Howard Schmidt, conseiller en Cyber Sécurité auprès de la Maison Blanche et Philippe Courtot, Chairman et CEO de Qualys, Inc.

Pour plus d'information, rendez-vous sur <http://www.csointerchange.org/>

Contacts presse :

Agence Tukilik

Adeline Lescale-Babel/Tommy Vaudecrane/Jeanne Moranne

Tel: 01 56 80 11 50

Mail: qualys@tukilik.com