CENTRE RISQUE & PERFORMANCE

POLYTECHNIQUE MONTRÉAL

Bulletin d'informations

Mai – juin 2014 Vol. 12 No. 3

Conférence du CRP / ASCQ / RECO-Québec

Des villes intelligentes et résilientes face à leur dépendance aux télécommunications?

Le lundi 2 juin, trois conférenciers présenteront leur vision de la problématique liée à l'utilisation grandissante des télécommunications en lien avec la continuité opérationnelle et la gestion des villes, des réseaux urbains et des entreprises :

- **Harout Chitilian, responsable du dossier de la ville intelligente, Ville de Montréal**
- **Marc Lapointe, directeur, Santé, sécurité et résilience, Bell Canada**
- **Luc Martineau, chef de division Ingénierie TRCP, Société de transport de Montréal**

La conférence gratuite aura lieu à Polytechnique Montréal. Une réservation est requise. Pour plus d'informations:

www.polymtl.ca/crp ou Irène Cloutier.

LES PARTENAIRES DU CRP :

Agence Métropolitaine de Transport, Bell Canada, Centre de services partagés du Québec, Gaz Métro, Hydro-Québec, Industrie Canada, ministère de la Sécurité publique du Québec, Recherche et développement pour la défense Canada, Sécurité publique Canada, Société de Transport de Montréal, Ville de Montréal (CSC, Réseau d'eau), Ville de Québec (BSC).

Ce bulletin est publié par le *Centre risque & performance* de Polytechnique Montréal. Si vous désirez que votre nom soit ajouté ou retiré de la liste d'envoi, communiquez avec : Irène Cloutier

Technologies de l'information : entre criminalité et vulnérabilité

La faille informatique Heartbleed a fait parler d'elle le mois dernier. En pleine période de déclaration de revenus sur Internet, l'Agence du revenu du Canada, au même titre que d'autres organisations, a été touchée par la découverte de cette faille, allant même jusqu'à interrompre ses services pendant quelques jours. Des possibilités d'atteinte à des données personnelles ont été largement évoquées par les médias faisant ressortir le terme de cybercriminalité. Cependant, au-delà de cette entorse à la vie privée, cet évènement met également en lumière un autre aspect moins évoqué publiquement : la vulnérabilité des organisations liée à l'utilisation grandissante des technologies de l'information (TI). En effet, depuis quelques années, la démocratisation de l'accès à l'informatique et la complexification des réseaux ont été des facteurs de développement du cybercrime, une des menaces qui pèsent sur le secteur des TI et par conséquent, sur toutes les autres organisations qui en dépendent.

Les pistes de recherche en matière de cybersécurité sont nombreuses. Parmi les dernières avancées connues, le National Institute of Standards and Technology (NIST) a publié en février dernier un rapport intitulé *Framework for Improving Critical Infrastructure Cybersecurity*. Ce document a pour but de rassembler, sur la base du volontariat, un ensemble de bonnes pratiques industrielles afin d'aider les infrastructures essentielles à gérer leurs risques cybernétiques. Quel que soit le secteur industriel auquel elle appartient, chaque organisation a la possibilité de dresser son propre profil de vulnérabilité et de s'améliorer continuellement à l'aide du guide. Au fur et à mesure, ce guide sera amélioré grâce aux feedbacks des organisations qui collaborent à la démarche.

Mais la vulnérabilité d'une infrastructure provient aussi des autres organisations dont elle dépend. À ce propos, TechAmerica conseille aux institutions gouvernementales de vérifier si leurs fournisseurs ont bien pris en compte la menace cybernétique sur leurs installations avant d'accorder un contrat (Rapport du CIP, avril 2014).

Cette démarche vise à instaurer, pour le secteur de la défense américaine, une chaîne d'approvisionnement collaborative face aux cybermenaces. Cependant, la multitude et la diversité d'acteurs en présence tout au long de la chaîne d'approvisionnement complexifie fortement la tâche.

Ainsi, au-delà de la chasse aux cybercriminels par les enquêteurs et des progrès en matière de méthodes d'investigation, les cyberattaques ne doivent pas faire oublier que les organisations, et en particulier les infrastructures essentielles, peuvent également agir en veillant à se protéger. Les attaques cybernétiques de plus en plus évoluées viennent sans cesse s'ajouter au lot de menaces qui pèsent sur les organisations et poussent celles-ci à s'adapter continuellement pour être moins vulnérables.

De la même façon, une autre vulnérabilité ne doit pas être sous-évaluée par les organisations, celle liée aux liens d'interdépendance complexes entre les réseaux de télécommunications. Les systèmes informatiques et téléphoniques ainsi que tout le réseau Internet dépendent du bon fonctionnement des réseaux de télécommunications. Au cours des prochaines années, un nouveau projet de recherche du CRP, en collaboration avec Industrie Canada, le Centre de services partagés du Québec et Recherche et développement pour la défense Canada, permettra de travailler sur la résilience de ces réseaux privés et publics. Dans un premier temps, l'accent sera mis sur l'établissement d'un cadre d'échange d'informations sensibles intersectoriel.

Dans le même ordre d'idée, la vulnérabilité face à l'utilisation grandissante des télécommunications est aussi liée à un autre concept plus récent qui viendra également toucher les organisations: celui de ville intelligente. Nouveau concept, nouvelles mesures, nouveaux besoins d'adaptation : les municipalités, les réseaux de télécommunications et les organisations sont-ils prêts à accueillir ces transformations ? Pour en savoir plus, n'hésitez à vous joindre à nous le 2 juin prochain (voir encadré ci-contre) !

Justine Arnoux, étudiante à la maîtrise, CRP