CYBERTERRORISME ET GESTION DES TIC DANS LES MUNICIPALITÉS

Patrick Champagne
Ministère des Affaires municipales, du Sport et du Loisir
Octobre 2004

SYNTHÈSE

Un groupe terroriste injecte une bactérie mortelle dans les prises d'eau potable de Montréal. Quelques minutes auparavant, l'un d'entre eux piratait le logiciel informatique de traitement des eaux de la municipalité et introduisait un virus dans le système de communication et de positionnement géographique des services d'urgence. L'infection se propage et les services d'urgence sont désorientés.

Fiction? À peine. Un article de Danny Krouk, publié dans le numéro de juillet 2004 de la revue *Planning*, nous apprend que le système de communication du service de police d'une ville du Midwest des États-Unis a récemment été interrompu pendant plus de cinq heures à la suite de l'attaque d'un virus informatique. Des perquisitions de caches en Afghanistan ont également permis de découvrir de la documentation sur un système informatique utilisé pour le traitement des eaux dans plusieurs villes canadiennes et états-uniennes. Dans les faits, le seul élément qui n'a pas encore été prouvé demeure l'existence d'armes bactériologiques ou chimiques…

Outre l'aspect dramatique d'un tel scénario, l'article de Krouk cherche surtout à démontrer que la sécurité informatique affecte la presque totalité des services à la communauté. Or, si les grandes entreprises et les gouvernements centraux ont bien intégré la dimension « sécurité » dans la gestion des technologies de l'information et des communications (TIC), il semble que les gouvernements locaux s'en soient peu souciés. Ce constat de Krouk rejoint d'ailleurs les résultats du sondage de la *National League of Cities*[1], qui démontrent que seulement 43 % des villes ont un plan d'urgence concernant le cyberterrorisme alors que 91 % d'entre elles craignent ce genre de terrorisme.

Certains gouvernements locaux, en réponse à de malencontreuses expériences ou suite à une prise de conscience de gestionnaires, se sont néanmoins attaqués à cet inévitable défi. Dans son article, Krouk présente les stratégies développées par le *Los Angeles County* de Californie et le *Truckee Meadows Waters Authority* du Nevada, qui ont choisi une approche intégrée et réaliste dans la mesure où les dirigeants ont pris conscience des risques, mais également des limites techniques, budgétaires et administratives.

Le défi : l'équilibre entre la sécurité et la productivité

L'attribut des gouvernements locaux qui influence le plus leur besoin en TIC, au même titre que pour plusieurs autres organisations publiques ou privées, est sans doute la diversité de leurs opérations. Pour les soutenir, les municipalités ont recours à une grande

[1] Voir Pierre Blais, *Le 11 septembre : les préoccupations des grandes villes américaines* [en ligne], ministère des Affaires municipales, du Sport et du Loisir, Observatoire municipal, janvier 2003, 2 p., http://www.mamsl.gouv.qc.ca/publications/obse_muni/grandes_villes_evenements_du_11_sept.pdf

variété de TIC, dont certaines permettent le travail à distance. Simultanément, plusieurs opérations telles l'information et les communications, se sont presque totalement informatisées. Pour répondre à cette nouvelle réalité, les stratégies de protection doivent nécessairement être diversifiées et ne peuvent être trop drastiques.

Puisque le but de la sécurité et des TIC dans une organisation est, en définitive, d'améliorer sa productivité, un système de sécurité ne peut être considéré comme efficace lorsque son coût ne rentabilise pas l'investissement des TIC qu'il protège ou lorsqu'il limite trop les capacités des TIC utilisées. Bloquer tous les accès extérieurs au réseau de la municipalité, par exemple, le protégerait totalement d'une intrusion, mais empêcherait par le fait même de profiter de nouvelles technologies fort avantageuses.

La gestion de la sécurité des TIC demande donc non seulement de protéger, mais de trouver un niveau de sécurisation qui justifie encore le recours aux TIC. Pour être efficace, la sécurité doit autant mettre l'accent sur les méthodes de protection que sur les activités de l'organisation, ses missions et ses opérations.

L'intégration des unités administratives

Il ressort des expériences examinées par Krouk que le succès de la mise en œuvre d'un projet de sécurisation de réseau informatique dépend, en premier lieu, de l'implication de l'ensemble des unités administratives. Chacune d'elles doit d'abord participer à l'identification des risques qui la concernent. Les mécanismes de protection de base peuvent alors être installés dans l'ensemble des services alors que des solutions raffinées et adaptées aux besoins spécifiques de chaque service sont implantées. Chaque unité doit également être invitée à participer à l'élaboration de lignes de conduite, à l'identification de bonnes pratiques et à la création d'équipes de répondants des incidents.

Il est également conseillé d'informer les employés de la part du budget consacrée à cette tâche. Une telle approche permet non seulement de développer des stratégies mieux adaptées, mais conscientise les employés à la problématique et permet éventuellement de faire accepter des décisions sujettes à controverse.

D'autres outils de protection

L'article nous rappelle également que la cybersécurité n'a pas nécessairement besoin d'être dispendieuse pour être efficace. Plusieurs gratuiciels sont reconnus pour leur grande efficacité et certains sites Internet mettent à la disposition des bibliothèques de bonnes pratiques ou d'exemples de politiques internes. Des interventions peu coûteuses, surtout au plan des habitudes de travail (politique interne d'utilisation du matériel informatique, copie de sauvegarde, prévention, formation des employés, partage de bonnes pratiques), permettent également de contrer un grand nombre de menaces.

Pour les municipalités de taille assez importante pour disposer de leur propre service d'informatique et de sécurité, Krouk ajoute qu'il peut être avantageux de se pencher sur les outils, les motifs et les pratiques des pirates informatiques. Certains logiciels

permettent maintenant de suivre les intrusions et d'étudier le comportement des pirates. Il est même possible d'engager une firme spécialisée qui tentera de s'infiltrer dans le réseau et rapportera ses vulnérabilités.

COMMENTAIRES

Cet article suscite l'intérêt puisqu'il met en évidence la mauvaise préparation de la majorité des municipalités états-uniennes, tout en proposant des solutions qui ne se limitent pas qu'à des dispositifs technologiques.

S'inspirer de l'évolution de la gestion des TIC

On retient que la finalité de la gestion de la cybersécurité est de choisir des méthodes de protection suffisamment fiables, parmi un éventail d'options, tout en préservant l'efficacité des opérations et l'atteinte des objectifs de l'organisation.

Il s'avère que les gestionnaires rencontrent ce défi dans l'ensemble de leurs décisions relatives aux TIC. Or, les analyses de l'évolution des TIC profitent d'un meilleur recul – les TIC ont fait leur apparition dans le monde du travail à la fin des années 1960. Il est donc intéressant de voir si les enseignements tirés de l'analyse de la productivité des TIC s'appliquent à la cybersécurité.

Spithoven, dans *The productivity paradox and the business cycle* (2003) se penche sur les raisons qui expliquent que le secteur des services n'a pas vu sa productivité augmenter malgré des investissements massifs dans les TIC depuis le début des années 1980.

Les hypothèses sont nombreuses :

- l'évolution rapide des technologies a demandé des investissements massifs pour constamment remplacer le matériel rapidement désuet;
- l'évolution rapide des technologies a nécessité des investissements importants dans la mise à jour des connaissances des employés;
- les employés dépassés par les changements rapides n'ont pas été en mesure d'utiliser les technologies à leur plein potentiel;
- la multiplication de la quantité d'information a ralenti le travail;
- de nouveaux phénomènes comme la flânerie sur Internet, les virus et l'utilisation à mauvais escient du matériel informatique sont apparus;
- les anciens modèles de gestion se sont avérés incompatibles avec les nouvelles réalités du travail informatisé.

Deux catégories de facteurs attirent particulièrement notre attention puisqu'ils peuvent inspirer la gestion de la sécurité informatique : l'évolution rapide des TIC et l'adaptation des mécanismes de gestion.

L'évolution rapide des TIC

Le premier impact de l'évolution rapide des TIC est d'ordre budgétaire. Contrairement à la majorité des investissements en équipement, les investissements dans les TIC ne peuvent s'amortir sur plus de cinq ans (en présumant que l'organisation se contentera de matériel désuet pendant deux ans!). De plus, si le coût des composantes électroniques, à capacité égale, a effectivement diminué, les besoins des organisations requièrent maintenant un matériel toujours plus performant. Bilan : la portion des budgets investie dans les TIC n'a pas diminué, contrairement à ce que plusieurs ont pu espérer.

L'évolution rapide des TIC a également entraîné un ensemble de coûts indirects. L'organisation qui investit dans les TIC en pensant voir sa production et ses profits augmenter risque souvent d'être déçue : « *This hope may, however, also be frustrated because computer technology is changing very fast and workers are constantly involved in acquiring new knowledge and solving problem cause by viruses and bugs in the software and hardware wich directly contribute to the production of final goods and services.* » (Spithoven, 2003 : 687).

Les mêmes constats s'appliquent à la sécurité – elle n'a pas d'autre choix que d'évoluer au même rythme que l'objet qu'elle protège! Il n'est pas possible de croire que les risques cesseront d'évoluer et l'arrivée de nouvelles technologies demandera l'implantation de nouvelles méthodes de sécurité. Comme tout autre outil informatique, les logiciels de protection demanderont de fréquents investissements pour être mis à jour et protéger de nouvelles failles. À la lumière de l'évolution des coûts des composantes et des logiciels, il semble aussi peu probable de voir le coût des technologies diminuer. Enfin, la rapidité des changements continuera d'affecter la performance des employés qui devront continuellement adapter leurs habitudes de travail.

L'adaptation des mécanismes de gestion

L'informatisation de la production demande des changements organisationnels. « *To gain advantage from computers in the workplace, rather than simply computerizing the traditional methods, managers have to re-engineer their company to match their business with the capabilities of computers. Computers need to be accompanied by a rethinking of the job process and of employee's roles and organizational hierarchy* » (Spithoven, 2003 : 687).

S'accompagnant généralement d'une augmentation de la scolarisation des employés, l'informatisation des opérations est peu compatible avec les approches de gestion centralisatrice, paternaliste et conservatrice de certaines grandes organisations. Cela rejoint les observations de Krouk qui constate que le succès d'une stratégie de protection repose sur la responsabilisation des employés et la prise en considération de leurs besoins par l'entremise d'actions à petite échelle.

Un tel constat prend encore plus d'importance dans le contexte d'un rajeunissement des ressources humaines. De par leur formation et la familiarisation à l'outil, qu'ils ont souvent acquises en bas âge, les jeunes ont développé une autonomie face à l'informatique qui peut potentiellement mal s'adapter à des modes de gestions centralisés

et contraignants. L'aversion des grandes organisations pour le changement, l'accroissement de la surveillance et de l'encadrement des actions de l'employé sont autant de facteurs qui peuvent avoir un impact sur la performance et entraîner des pertes de productivité.

D'un autre côté, Spithoven attire l'attention sur un phénomène délicat à aborder : la mauvaise gestion. « *An exemple for mismanagement can be when ICT investments are made although such investments are not in the best interest of the firm. This happen when managers simply mimic the investment decisions of other managers and ignore substantive information* » (Spithoven, 2003 : 688).

Les gestionnaires sont grandement sollicités, tant de l'intérieur de l'organisation que de l'extérieur, à moderniser et actualiser leurs opérations. Les alternatives technologiques sont nombreuses et complexes, et promettent souvent la lune. Rares sont cependant les gestionnaires et non spécialistes qui réussissent à maintenir à jour leurs connaissances dans le domaine. Généralement, ils appuient leurs choix sur l'expertise de spécialistes de l'informatique qui n'auront peut-être pas le réflexe d'examiner les possibilités d'opter pour des dispositifs de protection autres qu'informatiques.

Les connaissances limitées des gestionnaires permettent encore aujourd'hui aux TIC de profiter d'une certaine aura magique, d'une conception idéalisée. Plusieurs spécialistes ont su profiter du monopole de la connaissance et de la marge de liberté qui leur a été accordée pour augmenter leur pouvoir d'influence sur les décisions. Sans présumer de mauvais dessins aux spécialistes des TIC, l'on peut néanmoins croire qu'ils ont pu évoluer sans trop de critiques et sans l'apport de visions différentes et alternatives, d'une vision plus holistique. Spithoven illustre ce propos en démontrant comment plusieurs organisations ont investi massivement dans Internet pour offrir leurs services alors que leur clientèle n'était même pas branchée. Le temps de brancher la clientèle et d'intégrer dans ses habitudes l'utilisation du service en ligne, ce dernier était déjà désuet. Gain sur l'investissement : négatif.

Ce constat devrait inciter les gestionnaires qui doivent s'occuper de cybersécurité à mieux évaluer leurs besoins et les alternatives qui s'offrent à eux. Comme Krouk l'indique, les enjeux liés à la sécurité, comme pour l'ensemble de la gestion des TIC, ne sont pas que d'ordre technologique. Elles nécessitent une approche interdisciplinaire.

Autant en matière de sécurité, de matériel informatique ou d'outils Internet, les retours sur les investissements mériteraient d'être un peu mieux scrutés. Compte tenu des coûts, directs et indirects, que la sécurisation peut engendrer, il peut être intéressant pour les gouvernements locaux de réviser l'ensemble de leur stratégie informatique.

La recherche du progrès est toutefois une vertu difficilement contestable. Et quoi, plus que les TIC, représente actuellement mieux le progrès et la modernité? Quiconque s'inscrit à l'encontre des TIC risque rapidement de passer pour un conservateur ou même un réactionnaire, alors que d'un point de vue économique, investir dans les TIC n'est pas nécessairement garant d'une rentabilité.

À la lumière de tous ces constats, il ne faut pas conclure que la cybersécurité est sans importance, loin de là. Les municipalités sont responsables de protéger les données confidentielles et l'intégrité du matériel informatique, qui se rapporte notamment aux activités de protection des infrastructures sanitaires et de sécurité publique. Il faut toutefois se rappeler que le but de la sécurité est de protéger les TIC, qui ont pour but d'augmenter la productivité. L'efficacité de la cybersécurité repose alors sur sa capacité à soutenir ou améliorer la productivité de l'organisation.

RÉFÉRENCES

KROUK, D. « Cybersecurity at the Grass Roots », *Planning*, July 2004, pp. 14-18

SPITHOVEN, A. « The Productivity Paradox and the Business Cycle », *International Journal of Social Economics*, vol. 30, n°. 6, 2003, pp. 679-699