PRIMO
Public Risk Management Organisation

En collaboration avec

MARSH

COLLECTIVITES TERRITORIALES : COMMENT SE COUVRIR FACE AUX CONSEQUENCES D'UNE CYBER-ATTAQUE ?

Compte-rendu de la rencontre entre PRIMO, Marsh, Beazley et les Directeurs Généraux des Services invités – Octobre 2015.

Avant-propos

Primo (Public Risk Management Organisation), association créée en 2005 et dédiée à la gouvernance et à la gestion du risque dans le secteur public a vocation à informer, sensibiliser et aider les décideurs territoriaux dans le domaine de la gestion des risques a ici travaillé conjointement avec Marsh, leader de la gestion des risques et du courtage d'assurance. Le département secteur public du groupe Marsh est le partenaire des entités publiques locales et les accompagne dans l'analyse et le traitement de leurs risques. Primo et Marsh ont obtenu l'assistance et l'expertise de Beazley, assureur historique des risques cyber et membre des Lloyd's de Londres. Les connaissances et le travail quotidien des Directeurs Généraux des Services constituent la quatrième source de savoir nécessaire à la conduite de nos études.

Le 2 octobre dernier, l'association PRIMO France était présente au 75e congrès du SNDGCT à La Rochelle, en partenariat avec Marsh, afin de sensibiliser les acteurs du secteur public aux cyber-risques. Les Directeurs Généraux des Services sont au cœur des problématiques concernant la maintenance et la sécurité des données de leurs administrés et c'est pourquoi PRIMO a voulu aller à leur rencontre pour mener une enquête sur les besoins et le niveau de préparation des collectivités face à ces risques. La première initiative en ce sens a été menée l'été dernier : suite à l'envoi d'un questionnaire aux collectivités, les résultats ont été discutés dans un premier groupe de travail réunissant PRIMO, des acteurs privés du monde de l'assurance et trois DGS[1]. Les conclusions ont par la suite été compilées dans un rapport publié sur le site de PRIMO France[2].

Face au succès de cette première enquête, PRIMO et Marsh ont voulu saisir l'occasion offerte par le congrès du SNDGCT pour rencontrer de nouveau les DGS, et ainsi affiner leurs connaissances sur les besoins des collectivités locales quant aux risques cyber. Au-delà de son rôle d'étude, d'identification et de sensibilisation aux risques du secteur public, PRIMO a également la volonté de trouver le partenaire le plus pointu et le plus avancé sur un risque donné, puis d'en discuter avec les acteurs locaux afin de vérifier sa capacité à répondre correctement à leurs besoins. Ainsi, **Madame Emmanuelle Sagniez**, DGS de Calonne-Ricouart (Pas-de-Calais), **Monsieur Thibaut Barret**, DGS de Blandecques (Pas-de-Calais) et **Monsieur Tugdual Laouenan**, DGS de Bartenheim (Haut-Rhin) ont répondu présent à notre invitation et ont activement participé à un échange éclairant et constructif avec **Monsieur Gérard Combe**[3], Président de PRIMO France, **Thomas Graiff**, Responsable Secteur Public chez Marsh France et **Monsieur Jimaan Sané**, souscripteur en risques cyber-risques chez Beazley.

Cet avant-propos est également pour nous l'occasion de vivement remercier nos participants pour leur temps et leur implication lors de cette discussion.

---

[1] Il s'agissait de M. Patrice Girot, Président de l'Union régionale Ile-de-France du Syndicat national des directeurs généraux des collectivités territoriales et DGS de la Communauté d'Agglomération de la Vallée de Montmorency, M. Dominique Poey, Directeur Général des Services de la ville de Soisy-sous-Montmorency et Jérôme Couffy, DGS du Syndicat Intercommunal d'Etudes et de Réalisations d'Equipements d'Intérêt Général de la Vallée de Montmorency.

[2] « Les collectivités locales face aux conséquences du cyber-risque », septembre 2015.

[3] Président fondateur honoraire de l'Union des Dirigeants Territoriaux Européens (UDITE), Président national honoraire du SNDGCT, ancien DGS de la Ville de Nancy

Les conclusions du premier rapport

Il a été noté un réel manque de connaissances et de sensibilisation des collectivités et de leurs agents quant à aux cyber-risques. Bien que bon nombre d'entre elles fassent preuve de bonne volonté, les collectivités peinent à atteindre un niveau minimal de protection des données ; quand bien même elles auraient mis en place une prévention renforcée (SSI, antivirus, firewall, cryptage…), presque aucune aujourd'hui n'est couverte face aux conséquences du cyber-risque.

Les acteurs privés du secteur informatique poussent visiblement les collectivités à centraliser leurs données tout en les délocalisant, exposant ainsi les collectivités à un risque accru et nécessitant une protection adaptée et efficace afin de limiter les conséquences d'une éventuelle attaque.

Entre 2014 et 2015, on a pu constater l'augmentation significative des cyber-attaques envers les collectivités territoriales, avec un net pic de progression suite aux attentats de janvier dernier. Malheureusement, l'augmentation des impératifs numériques et les évolutions techniques ne présagent qu'une accélération de la fréquence de ces attaques envers les collectivités, qui peuvent aller du défacement à la prise en otage de données. Ces attaques peuvent avoir une conséquence désastreuse sur la gestion interne des collectivités, le principe de continuité du service public et sur l'image de la collectivité elle-même et de ses élus.

L'ENQUETE PRIMO/MARSH EN QUELQUES CHIFFRES

15%	***10%***	***35%***	***10%***
des collectivités ont fait concevoir leur site par un agent	*ne connaissent pas la paternité de leur site*	*avouent héberger des données sensibles*	*organisent des formations de sensibilisation pour leurs agents*

Discussion

Des données sensibles et exposées

Au cours de cet échange, il est rapidement ressorti qu'une majeure partie des données détenues par les collectivités pouvait être qualifiées de « sensibles ». En effet, les services de gestion du personnel et des paies ont en leur possession des informations tout à la fois nécessaires à leur bon fonctionnement et absolument confidentielles : montant du salaire, adresse, numéro de compte sont autant d'informations précises et chiffrées qui appartiennent strictement à la sphère privée.

Les Centres communaux d'actions sociales (CCAS) sont également des centralisateurs d'informations personnelles qui ne sauraient souffrir d'aucune divulgation. Le CCAS est amené à réaliser une collecte d'informations sociales afin d'assurer une traçabilité des situations personnelles : ils détiennent ainsi de nombreuses données relatives à la composition des foyers, aux revenus, ou encore aux prestations et aides sociales dont certains administrés peuvent être les bénéficiaires.

Le cas des données cadastrales a également été évoqué. Ce référencement précis du territoire de la commune comporte bon nombre d'informations personnelles telles que le relevé précis des constructions qui se trouvent sur chaque parcelle, leur évaluation fiscale et la désignation du propriétaire.

Les services d'Etat civil sont également détenteurs de documents sensibles quant à l'identité et la situation personnelle des administrés. Aujourd'hui, la majorité des actes d'Etat civil sont édités de façon numérique et sont issus de données conservées sur le réseau. La mise en place du « guichet unique » tend à se généraliser dans les collectivités territoriales, démarrant ainsi une vague de centralisation des données en un seul point. Les administrés pourront ainsi réaliser en ligne leurs démarches sociales, scolaires, fiscales ou autres selon les choix de la Commune. Les outils en ligne de ce guichet permettront également de procéder aux paiements de toute nature, ajoutant les données bancaires à toutes les informations sociales et fiscales du guichet unique.

L'un de nos invités a par ailleurs souligné qu'un *phishing* (ou hameçonnage) s'était déjà produit au sein de sa collectivité. Ce type de piratage insidieux ne s'attaque pas directement aux données détenues par la collectivité mais, en passant par les serveurs de l'entité, les pirates se font passer pour elle afin d'obtenir des informations confidentielles de la part des administrés.

Enfin, en abordant la thématique de la sauvegarde et de la conservation de ces données, un double problème est apparu, confirmant l'une des conclusions de notre première enquête. En effet, les collectivités ont tendance à centraliser toutes leurs données sur un serveur unique, multipliant par là même et de façon exponentielle la lourdeur des conséquences d'une cyber-attaque. Pourtant, alors que les prestataires du secteur informatique conseillent de décentraliser les données et de les conserver sur plusieurs serveurs différents, cette pratique induit nécessairement la sauvegarde à distance éloignant ainsi les données du contrôle de la collectivité et les exposants à un autre risque de piratage ou de perte.

Un phénomène bloquant pour les activités courantes

L'exemple d'une collectivité de la région Rhône-Alpes dont les serveurs ont été bloqués pour protester contre l'installation de la ligne de train Lyon-Turin, met en évidence tous les dommages collatéraux relatifs à l'impossibilité d'utiliser l'intranet et les systèmes internes de la collectivité.

Ainsi, en bloquant les serveurs, la communication interne devient presque impossible : l'accès au réseau, les mails et éventuellement certaines lignes téléphoniques qui passeraient par un routeur se trouvent totalement gelées. L'accès aux documents dématérialisés et aux ressources contenues sur le serveur est alors impossible, entravant ainsi la réalisation des tâches quotidiennes nécessaire au bon fonctionnement de la collectivité. Il est alors possible, au vu de certaines compétences spécifiques dont peuvent être investies les collectivités, de faire face à des pertes financières consécutives à la perturbation de leur activité.

Les systèmes de gestion interne utilisant le réseau s'en trouvent également stoppés net : ressources humaines et matérielles, versement des salaires, alarmes, système de surveillance et PC sécurité pourraient être considérablement impactés par le blocage des serveurs de la collectivité. De plus, le cas du piratage du site du Conseil Général du Tarn en 2014 et en 2015, a prouvé que le hacker

pouvait, par capillarité, avoir accès à tous les sites affiliés à celui de la collectivité piratée. Ainsi lors de ce piratage, une trentaine de sites dépendant du département ont été bloqués en une seule attaque, notamment les sites des musées, des archives ou celui relatif aux zones humides.

Des conséquences coûteuses

L'un des dirigeants invités a eu l'occasion de relater son expérience de la perte de données survenue récemment dans sa collectivité. L'incident a nécessité un travail de longue haleine et une énergie colossale, mobilisant de nombreux acteurs de la collectivité. Les coûts engagés ont été particulièrement élevés : face à l'urgence de la situation, toutes les solutions proposées ont été tentées, sans pour autant n'avoir aucune certitude sur leur efficacité.

Car en effet ce type d'incident entraîne d'importants coûts de réparations, d'honoraires pour conseils, et d'éventuels frais suite aux réclamations des tiers lésés. Jimaan Sané de l'assureur Beazley a par ailleurs souligné la différence de risque entre l'attaque idéologique et l'attaque crapuleuse. La première est généralement une réponse à un projet ou un événement récent, et nécessite du hacker une mise en place rapide et donc, peu organisée et peu précise. De plus, ces attaques sont généralement conçues pour être vues par le plus grand nombre, et sont *de facto* facilement détectables. En revanche, l'attaque crapuleuse vise à soutirer des informations ou de l'argent à la cible et nécessite d'être extrêmement préparée et très sophistiquée ; en cela, elle est particulièrement difficile à détecter, et peut se produire sur un temps particulièrement long.

Les répercussions d'une telle attaque sur l'e-réputation de la collectivité et de ses élus sont nombreuses. Tout d'abord, la nature de l'attaque peut elle-même viser à entacher l'image d'une structure, de ses dirigeants ou de ses élus, par l'affichage de messages revendicatifs ou injurieux. Ensuite, les administrés seront amenés à juger la façon dont la collectivité a géré cet événement : a-t-elle été réactive et efficace ? Enfin, il sera attendu de la part des administrés une phase de communication concrète sur le pourquoi et le comment de la chose, dans laquelle la collectivité devra rendre compte de ses erreurs et faire amende honorable, nécessitant une gestion de crise rapide et efficiente. Il ne faut pas oublier que l'événement pourra également faire l'objet d'une couverture médiatique de plus ou moins grande ampleur en fonction de la collectivité et de la gravité de l'attaque et que d'aucuns y trouveront une bonne occasion de récupération politique.

La problématique centrale du budget des collectivités a été abordée ; en effet, les baisses de dotations de ces dernières années et celles qui s'annoncent entre 2015 et 2017 resserrent de plus en plus l'étau autour des finances locales. Certaines structures pourraient donc avoir tendance à évacuer *ipso facto* l'éventualité d'une couverture quant aux conséquences que nous avons évoquées. Attention cependant, car les sommes

engagées par les réparations et honoraires, la gestion de crise, les réclamations des tiers et d'éventuelles pénalités atteignent un montant nettement supérieur au prix de la police cyber, qui elle, prendrait tout en charge. De plus, les critères de calcul de la prime se basent sur la taille de la collectivité, tendant intrinsèquement ainsi à suivre les capacités budgétaires de celle-ci.

Conclusion

Il est apparu plutôt clair que les cyber-risques pouvaient toucher n'importe quelle collectivité au vu de la diversité des types d'attaque et des motifs. L'étendue des impacts sur la gestion courante et la lourdeur des coûts sont des raisons suffisantes pour ne pas attendre que l'événement arrive pour se couvrir. Ces conséquences, qui se sont révélées nombreuses et diverses, sont par nature difficiles à gérer pour une collectivité, d'où la nécessité d'avoir un accompagnant qui puisse également financer les coûts.

Les Directeurs Généraux des Services et les élus sont parfois en retrait par rapport aux SSI, bien qu'ils soient en première ligne en cas d'incident. La mise en place d'une police cyber intègre une phase importante de diagnostic, qui permet de faire la lumière sur les forces et les faiblesses des systèmes mis en place, et donc de donner à chacun une visibilité sur ces installations très techniques.

Dans tous les cas de piratage, la collectivité sera toujours responsable des conséquences de la cyber-attaque : elle est la gardienne des données personnelles de chacun, et elle en assume toutes les conséquences aux yeux de la loi. La responsabilité pénale des élus est engagée en cas de négligence, et la jurisprudence est implacable s'il est avéré que les élus n'ont pas suffisamment agi pour protéger systèmes d'informations et données. Certaines collectivités sont conscientes des risques, mais il faut de toute urgence faire passer cette prise de conscience en perspectives managériales.

La police cyber offre une présence constante de l'assureur, ne serait-ce que pour lever un doute ou répondre à une incertitude. L'assureur est ici un accompagnant avant, pendant et après l'incident, jusqu'au rétablissement d'image par la communication et la gestion de crise.

Primo France est une association dont la vocation est d'accompagner les responsables publics en matière de gestion des risques. Créée en 2005 sous l'égide de l'UDITE (Union Des Dirigeants Territoriaux Européens), elle compte parmi ses membres fondateurs le SNDG, Syndicat National des Directeurs Généraux des Collectivités Locales (3500 DGS), des entreprises du secteur privé (Marsh, Dexia, RM Partners). Son but est d'insuffler une culture de la bonne gouvernance du risque, l'un des plus grands défis du secteur public local.

MARSH S.A.S.
Société de Courtage d'Assurances
Société par Actions Simplifiée
Capital 5.807.566,00 Euros
RCS Nanterre : 572 174 415
N° ORIAS 07 001 037 – www.orias.fr
N° TVA intra-communautaire :
FR 05 572 174 415
Assurance de responsabilité civile professionnelle et Garantie financière conformes aux articles L512.6 et L512.7 du code des assurances.

Marsh, leader mondial du courtage d'assurance et du conseil en risques d'entreprises, emploie 26 000 collaborateurs et propose à ses clients des capacités d'analyse, de conseil et de transaction dans plus de 100 pays. Marsh est membre du Groupe Marsh & McLennan Companies (MMC), un groupe de services professionnels et financiers qui emploie près de 55 000 collaborateurs et dont le chiffre d'affaires dépasse les 11 milliards de $.
MMC est aussi la société mère de Guy Carpenter, spécialiste du risque et de la réassurance ; Mercer Human Resources Consulting, conseil en ressources humaines ; et Oliver Wyman, conseil en stratégie. MMC est coté en Bourse à New-York, Chicago et Londres.