PRIMO
Public Risk Management Organisation

En collaboration avec
MARSH

LES COLLECTIVITES LOCALES FACE AUX CONSEQUENCES DU CYBER RISQUE

SEPTEMBRE 2015

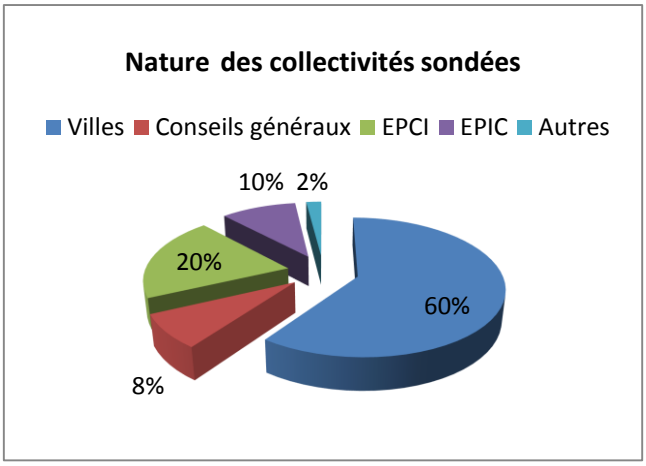
INTRODUCTION, METHODOLOGIE

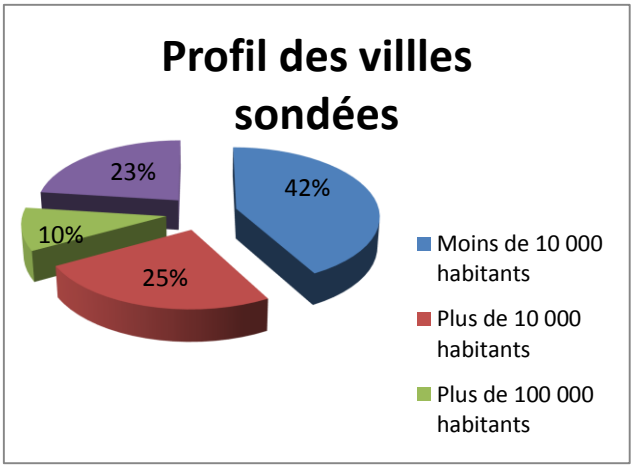
Primo France, association dédiée à la gouvernance et à la gestion du risque public, a conduit une enquête portant sur l'exposition des collectivités publiques locales au cyber risque.

Pour mener à bien cette analyse, une première réflexion a été menée au sein de Primo France, où étaient réunis autour de M. Gérard Combe[1] : MM. Patrice Girot[2], Dominique Poey[3] et Jérôme Couffy[4].

Par la suite, un questionnaire en ligne a été envoyé à une centaine de collectivités françaises, villes et intercommunalités, portant sur l'exposition de ces dernières au cyber risque et à ses conséquences.
Parmi elles, 60% sont des villes, 8% sont des Conseils Généraux, 20% sont des EPCI, 10 % sont des EPIC et 2% d'autres catégories.

42% des villes interrogées ont une population de moins de 10 000 habitants, 25% sont des villes de plus de 10 000 habitants, 10 % sont des villes de plus de 100 000 habitants. Les 23% restants n'ont pas souhaité renseigner leur population.





[1] Président de Primo France

[2] 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

[3] Directeur Général des Services de la ville de Soisy-sous-Montmorency

[4] DGS du Syndicat Intercommunal d'Etudes et de Réalisations d'Equipements d'Intérêt Général de la Vallée de Montmorency

Les résultats de l'étude ont ensuite été discutés dans le cadre d'un groupe de travail, dont faisaient partie, en plus des membres du groupe de réflexion nommés plus haut : M. Thomas Graiff, responsable du Secteur Public au sein du groupe Marsh, ainsi que deux collaborateurs de l'assureur Beazley : Mme Julia Popper, directeur de développement pour la France et M. Jimaan Sané, souscripteur en cyber risque.
La volonté d'analyser la façon dont le risque cyber est géré par les collectivités locales s'inscrit dans la continuité des études réalisées par Primo France et Marsh depuis 2005.

Primo France, grâce à sa collaboration avec Marsh peut régulièrement enquêter auprès des DGS afin de déterminer les évolutions de la gestion des risques au sein du secteur public local.

L'édition 2015 met en avant les risques liés à l'ultra-connectivité des collectivités, et aux données sensibles dont elles ont la garde.

Gérard COMBE
Président de Primo France

Les enseignements suivants sont à retenir :

- Les directeurs généraux des services, par leur vision transversale, restent les acteurs les plus impliqués en matière de gestion des risques ;

- Malgré une sensibilité aux risques qui ne cesse de croître, les mécanismes mis en place pour la gestion des cyber risques demeurent insuffisants ;

- L'exposition croissante des collectivités aux risques cyber est due, d'une part, à l'augmentation des accès connectés en interne et en externe (guichet unique, sites des collectivités, données sensibles, etc.) et, d'autre part, à la montée d'un terrorisme cyber, idéologique ou purement mercenaire.

- L'achat d'assurance reste encore un outil de protection* peu utilisé par les collectivités qui appréhendent surtout des freins politiques, techniques et réglementaires liés à sa mise en œuvre.

** l'assurance est une protection puisqu'elle permet de diminuer l'impact du risque encouru.*

LA GESTION DU CYBER RISQUE AU SEIN DES COLLECTIVITES FRANÇAISES : ETAT DES LIEUX

En comparaison des résultats des enquêtes précédentes, on notera **une prise de conscience** des collectivités de l'importance des problématiques liées au cyber risque.

Par rapport aux entités du secteur privé comptant le même nombre de salariés, les entités publiques accusent néanmoins un certain retard en la matière. Les collectivités locales, quel que soit leur poids économique et démographique, gèrent et possèdent de nombreuses données confidentielles, sensibles et privées, qu'il convient de protéger des malveillances. Près de 20 000 sites internet français ont subi des attaques depuis les attentats de Charlie Hebdo, selon le journal Ouest France, daté de Mars 2015.

Quels sont les risques liés au cyber?

L'étude préalable menée par Primo France depuis 2014 indique que trois aspects sont à prendre en compte dès lors qu'on aborde le sujet du cyber : confidentialité, intégrité et disponibilité des données. On trouve également trois types de cyber-agresseurs : le cyber pirate purement mercenaire, l'agresseur idéologique ou le cyber espion. Les deux premiers agresseurs sont les plus susceptibles d'attaquer les sites et les données des collectivités.
Le premier pour en tirer une rançon quelconque, et le deuxième pour mettre à mal l'image de la collectivité.
Le troisième cyber-agresseur ne concernerait que les organisations de l'Etat, notamment pour pirater des données classées Secret Défense.

Les types d'attaques varient en fonction des agresseurs et de leurs compétences techniques. Néanmoins, il convient de préciser que toutes les attaques commises, quelles que soient leur degré, gêneraient les collectivités victimes.

Les différentes agressions :

- **Défiguration** (ou **défaçage**) du site public d'une collectivité, le rendant illisible aux internautes ;

- **Vol de données confidentielles**, **sensibles**, **privées** contre une demande de **rançon** ;

- **Attaque en déni de service** : mode opératoire consistant à bloquer l'accès aux serveurs, empêchant le bon fonctionnement d'un ou plusieurs services ;

- **Sabotages** divers entraînant la **perte** pure et simple **de données**.

Quelles conséquences pour les collectivités ?

Les suites de ces attaques peuvent être plus ou moins graves, mais entacheront quoi qu'il arrive l'e-réputation des collectivités. L'image renvoyée aux administrés sera renforcée négativement et, par ramification, aura un impact sur une future élection.

L'attaque la moins grave, à savoir la défiguration d'un site, entraîne des répercussions moindres que les autres sur l'image de l'administration et sa réputation. Cependant, la hausse de ces attaques et leur virulence doivent accroître la vigilance des collectivités concernant leur site, qu'il soit transactionnel ou non.

Concernant le vol ou la perte de données sensibles ou confidentielles, les conséquences en sont plus graves : publications de données privées pour mettre à mal l'image de l'entité territoriale, revente à un tiers, ou encore prise en otage des données contre une demande de rançon, les malfaisances liées à ce méfait sont nombreuses et ont des suites pénibles pour les entités et les équipes victimes.

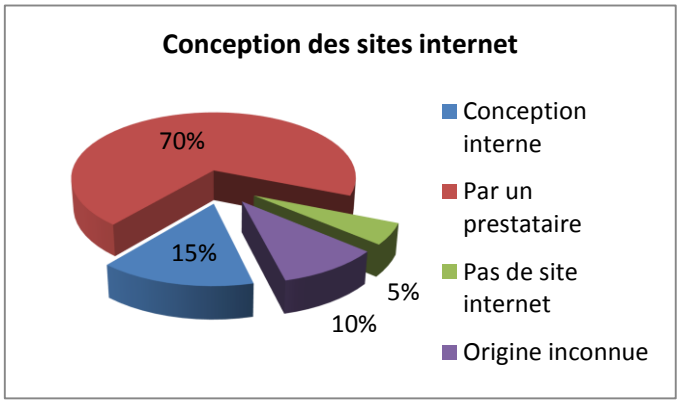
Quant à l'attaque en déni de service, elle est plus grave : d'abord, parce que le hacker n'est pas toujours un spécialiste et peut détruire d'autres données, par une mauvaise manipulation. Lorsqu'elle est orchestrée par un pirate aguerri, elle n'en est pas moins grave : celui-ci a tout pouvoir pour faire repartir le système ou l'arrêter indéfiniment.

En ces périodes d'hyper-connectivité des

équipements municipaux, ce type d'attaque est très à la mode et empêcherait le bon fonctionnement de nombreux services : eau, électricité, circulation, etc.

De plus, les collectivités possèdent de nombreuses données, sensibles ou privées : coordonnées bancaires, données personnelles sur élus et/ou administrés, informations de santé, informations sociales ou financières, liste d'élus, etc. Que faire si ces données tombent entre de mauvaises mains ? Leur revente ou leur divulgation publique aurait des répercussions encore mal connues, forcément étendues dans le temps et compromettant toute l'équipe en place.

Les collectivités sont-elles préparées?



On constate, sur l'ensemble des réponses des sondés, une conscience du danger qu'impliquent les nouvelles technologies et leur utilisation au quotidien dans les services publics.

Cependant, les équipes demeurent insuffisamment préparées : très peu suivent les recommandations du Référentiel Général de Sécurité et de la CNIL, des étapes pourtant essentielles pour un embryon de mise en place des processus informatiques.

15% des sondés ont déclaré que le site internet public de leur collectivité était créé par un agent, contre 70% passés par un prestataire. 5% des sondés n'ayant pas de site internet, il reste donc 10% des sondés qui ne sont purement et simplement pas au courant de la paternité du site sur lequel sont postés des informations.

Deux formes de sites internet sont ici à prendre en compte :

- les simples sites dits « plaquettes », qui ne font que présenter des informations publiques (horaires, équipes, téléphone, etc.), qui seront surtout sujets à des campagnes de défiguration de la part des hackers. Ils peuvent cependant représenter une brèche d'intrusion pour les hackers, pour peu que les serveurs soient communs et que le site soit alimenté depuis la mairie sans protection particulière.

- les sites transactionnels, où l'administré peut interagir sur son compte personnel (demandes administratives diverses : attestations, inscriptions à des services ou activités de la mairie, par exemple, crèche ou autres accueils périscolaires). Sur ces sites, non-seulement la collectivité est plus vulnérable, puisque les ponts de connexion se font plus facilement, mais en plus, les victimes collatérales peuvent donc être des tiers, des administrés dont on usurpe l'identité électronique pour accéder au guichet unique. En ces cas, la collectivité devra bien entendu régler la crise en interne et en externe, avec un risque accru de perte de réputation.

On constate, sur l'ensemble des collectivités interrogées, une méconnaissance de leur propre parc et réseau informatique : moins de 15% des sondés ont pris connaissance du Référentiel Général de Sécurité (RGS), pourtant indispensable lors de la création d'un site. 15% des sondés font part de leur connaissance de l'existence d'un Correspondant Informatique et Libertés (CIL) ou d'un agent responsable de la protection des données. Les 85% restants ne savent tout simplement pas s'il existe un agent alloué à cette problématique.

10% des sondés seulement organisent des formations de sensibilisation pour leurs agents, et un peu moins de 13% utilisent des procédures de révocations des comptes professionnels de leurs agents une fois que ceux-ci ont quitté leurs fonctions.

Quant au cryptage des données, aucune collectivité interrogée n'y a recours : 5% des sondés ne savent tout simplement pas si cette possibilité existe, les 95% restants ne l'utilisant pas.

Et pourtant, près de 35% des sondés avouent héberger des données sensibles, voire privées, sur administrés et/ou élus.

Les collectivités interrogées sont pourtant bien conscientes des torts que pourrait engendrer une cyber-attaque, mais ne se donnent pas encore les moyens de se protéger des conséquences d'une telle attaque.

LES COLLECTIVITES SONT-ELLES PRETES A ASSUMER LES CONSEQUENCES D'UNE CYBER ATTAQUE ?

Entretien exclusif avec M. Jimaan Sané, souscripteur cyber-risques chez Beazley

Beazley est un groupe international d'assurances spécialisées, opérant en Europe, aux Etats-Unis, en Asie et en Australie. La société mère, Beazley PLC, cotée à la Bourse de Londres, gère cinq syndicats du Lloyd's et a souscrit, en 2012, $1,896 million de primes brutes. Présent en France depuis plus de 10 ans, Beazley propose une large gamme de produits RC Professionnelles, Responsabilité des Dirigeants, Responsabilité Médicale et Cyber Criminalité, conçus pour s'ajuster sur mesure aux besoins pointus de leurs clients et aux particularités de leur activité.

Les attentats de janvier 2015 et les centaines de piratages de sites de collectivités qui ont suivi en France, ont rappelé combien elles pouvaient être exposées aux risques informatiques.

Ces attaques, réduites pour l'instant au défaçage de sites Internet, visent essentiellement la diffusion de messages politiques. Mais quid demain d'une intrusion dans le réseau informatique d'une collectivité, en vue d'un vol massif d'identités ?

Avec la numérisation croissante des documents administratifs, les collectivités ont en possession un vivier d'informations personnelles, à commencer par l'état civil de leurs concitoyens, leurs justificatifs de domicile, leurs données fiscales ou encore les inscriptions en établissements scolaires et périscolaires … Quand ce ne sont pas les résultats d'un vote électronique lié à un projet municipal.

Par manque de budget, d'expérience et souvent de compétences, dans ce domaine, **les collectivités locales ne sont globalement pas assez protégées pour faire face à la menace de piratage.** Quand elles disposent d'un responsable informatique, il porte également la casquette de RSSI, avec à sa disposition des moyens nettement inférieurs à ceux du secteur privé. Au déficit de protection, s'ajoute le manque de formation du personnel aux risques informatiques. Comme dans toute entreprise, **le premier facteur d'une violation de données reste l'erreur humaine**. Sur les 1500 sinistres que notre compagnie a indemnisés entre 2013 et 2014 dans le monde, plus de cinquante pour cent des cas étaient issus soit d'une divulgation accidentelle d'informations, par e-mail notamment, soit de la perte de documents physiques.

En l'absence de directives européennes, le cadre réglementaire relatif à la sécurité des systèmes d'information est d'origine jurisprudentielle. Au même titre qu'un chef d'entreprise, **le maire d'une commune est susceptible d'être mis en examen pour n'avoir pas pris les mesures de protection nécessaires.** Si **les cas de sanctions juridiques**, bien que possibles, sont encore rarissimes, c'est en revanche sur le plan de l'image que les retombées peuvent être les plus préjudiciables. Les cas de fuites de données exposent les entreprises à **un important déficit de réputation**, dont l'impact commercial peut s'avérer catastrophique. Ainsi, une étude internationale menée auprès de consommateurs de 24 pays a révélé que 38 % des personnes victimes d'une violation de données déclaraient avoir cessé de traiter, en conséquence, avec l'organisation concernée.

Dans le cas d'une collectivité, s'il est plus compliqué de changer de ville ou de région, il est en revanche envisageable de **sanctionner ses élus par le vote**. Selon l'importance et la gravité du sinistre, **la confiance en l'équipe municipale peut, en effet, très vite se détériorer**.

Face à la numérisation croissante des données, pour des raisons premières de facilité de service, et face à la montée des menaces d'intrusion, **les collectivités locales doivent prendre la mesure des risques qu'elles font prendre à leurs administrés**.

Parce qu'en matière de cyber sécurité, le risque zéro n'existe pas, il est de la responsabilité des élus d'agir, en premier lieu, sur leur capacité à pouvoir réagir vite et contenir les effets d'une perte massive de données. Ceci implique de pouvoir **mettre en place rapidement une cellule de crise**, orchestrant l'intervention en urgence d'experts informatiques, dans le but de corriger la faille du système et de surveiller le web à la recherche des données subtilisées. Une cellule de crise **permet également d'informer le plus tôt possible les administrés concernés par le vol d'identités et de les rassurer sur les moyens mis en œuvre.**

Ces dernières années, la plupart des assureurs spécialisés dans les cyber-risques ont mis au point un service de gestion de crise externalisé, mobilisable en urgence. Nul doute que ce type de support, qui a déjà fait ses preuves auprès des entreprises, deviendra à l'avenir un partenaire de premier plan pour les collectivités dans leurs réponses aux attaques informatiques.

CONCLUSION

Le contexte cyber est encore jeune, puisque les principales attaques médiatisées datent pour la plupart de moins d'un an. On ne peut qu'anticiper une augmentation de ces attaques et de leurs conséquences.

Cependant, le constat est bien présent : les collectivités, bien que pleines de bonne volonté, peinent à atteindre un niveau minimal de protection de leurs données, et sont, de fait, mal préparées aux futures révolutions apportées par le guichet unique et la ville connectée.

Les acteurs privés du secteur informatique poussent à centraliser les données, tout en les délocalisant (Cloud, gestion électronique à distance, etc.), envoyant ainsi des signaux contradictoires et exposant les collectivités locales à un risque accru, nécessitant la mise en place d'une couverture efficace afin de de réduire les conséquences néfastes d'une cyber attaque.

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.

PRIMO
Public Risk Management Organisation

Enquête sur la gestion
des risques cyber par les collectivités locales
Réalisée au 2ème semestre 2015
www.marsh.fr
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.
Les informations figurant dans la présente publication ont uniquement vocation à aborder les thèmes concernés de manière générale et n'ont nullement valeur de conseil personnalisé. Par conséquent, il convient de ne pas utiliser ces informations en tant que telles. Marsh est à votre disposition pour étudier vos besoins spécifiques. Ni le présent document, ni aucune partie des informations qu'il contient ne peuvent être copiés ou reproduits sous aucune forme que ce soit sans le consentement de Marsh S.A.S., à l'exception des clients de Marsh S.A.S. qui ne sont pas tenus d'obtenir ladite autorisation pour tout usage du présent document à des fins internes.

En collaboration avec

MARSH