La lettre d'Intelligence Économique et Territoriale de l'EM Normandie – N°20

Comprendre & Entreprendre

Se développer dans un monde complexe

Les collectivités territoriales et leurs écosystèmes au défi des nouveaux risques numériques

Rémy Février

Professeur-associé à l'EM Normandie, docteur en sciences de gestion et maître de conférences au Conservatoire national des arts et métiers (CNAM), Rémy Février, expert en intelligence économique et sécurité des systèmes d'information, est l'un des meilleurs connaisseurs des questions de cybersécurité dans notre pays. Ancien officier supérieur de la Gendarmerie nationale en matières de risques numériques, il livre ici les leçons tirées de son expérience, tant dans les entreprises que vis-à-vis des services de l'Etat et des collectivités territoriales.

Dans l'entretien qu'il a accordé à Jean-Guy Bernard, Directeur Général de l'EM Normandie, Rémy Février pointe les risques majeurs auxquels se trouvent confrontées les collectivités territoriales, en particulier dans leurs relations avec leur environnement social et économique. Au-delà des spécifications techniques, il rappelle surtout que c'est une réelle prise de conscience que doivent avoir, à tous les niveaux de responsabilité, élus, fonctionnaires et autres décideurs. Les risques numériques vont sans cesse croissant. L'ignorer, c'est se condamner à se faire piller, donc à perdre dans la guerre économique.

Vous êtes reconnu comme l'un des meilleurs spécialistes français en matière de cybersécurité des collectivités locales. Où en sommes-nous aujourd'hui ? *Quid* de la prise de conscience de l'ampleur des risques ?

Avant toute chose, je crois important de réaliser un rapide état des lieux. La conclusion de ma thèse de doctorat - qui a porté sur le sujet - est qu'il existe une véritable inconscience de la part des responsables de collectivités vis-à-vis de ces menaces. Nous avons malheureusement tendance, en France, à sous-estimer les risques au sens large, *a fortiori* les menaces numériques. Il faut donc savoir que recueillir des données fiables sur la cybersécurité se révèle délicat. Pour aborder la thématique spécifique des collectivités territoriales, il est fondamental de mettre en évidence le fait selon lequel ces dernières se situent à la conjonction de trois univers : politique, économique et sociétal. Les maires se retrouvent ainsi, à leur corps défendant, à l'intersection de ces trois mondes, lesquels ne se connaissent pas forcément bien, s'ignorent parfois et se défient l'un de l'autre le plus souvent. Or, pour ceux qui président aux destinées des collectivités territoriales, il est fort risqué lorsque l'on s'exprime, tant de reconnaître que l'on s'est fait "hacké" que d'avouer que l'on n'y comprend rien…

Et pourtant, il n'est pas un jour où les médias ne rapportent des cas de piratage, à plus ou moins grande échelle, portant tant sur la sphère publique que privée. Mais rien n'y fait. On observe sur notre territoire un manque flagrant de prise en compte des risques numériques à destination des collectivités, tant de la part des élus que des fonctionnaires territoriaux. A cet égard, curieusement, la taille de la collectivité n'est pas toujours un critère déterminant. Tout dépend, en fait, de la prise de conscience du président de l'exécutif local quant au risque numérique et de sa capacité à prendre en compte les analyses de son DSI [Directeur des systèmes d'information]. Si c'est le cas, il va agir, avant tout pour se protéger, en même temps qu'il va protéger la structure à la tête de laquelle il a été élu.

Comprendre & Entreprendre

De par sa vocation, l'EM Normandie entretient un lien puissant avec son territoire et les entreprises qui s'y développent. D'où sa légitime implication dans les enjeux relevant de l'Intelligence Économique et Territoriale. Car c'est ici, sur notre sol, que s'enracinent les projets qui assureront demain notre prospérité.

La lettre de réflexion Comprendre & Entreprendre vise à soutenir cette dynamique. Elle s'adresse à toutes celles et ceux qui anticipent, imaginent l'avenir et doivent faire des choix stratégiques. Seule la combinaison astucieuse de l'action et de la réflexion nous permettra d'optimiser notre positionnement et notre engagement au sein d'un monde complexe et mouvant.

De par leur importance et la quantité croissante de données dématérialisées qu'elles gèrent, il est inquiétant de constater le niveau insuffisant de protection des collectivités locales en matière de cybersécurité ! D'autant que ces failles peuvent également avoir des conséquences directes pour les entreprises travaillant sur le territoire ou en lien avec lui…

Dans le secteur privé, le critère essentiel qui va déterminer l'attaque contre une entreprise n'est plus sa taille ou son secteur d'activité mais sa capacité d'innovation.

Vous avez tout à fait raison. Prenons un exemple simple pour bien saisir l'ampleur du problème : celui des ordinateurs en fin de vie. Se pose la question de la confidentialité de leurs contenus, à savoir comment supprimer définitivement les données - au travers d'une destruction physique ou d'un nombre suffisant de reformatages successifs - avant de les envoyer au rebut… Savez-vous combien de fichiers à caractère sensible et personnel existent dans l'informatique d'une une collectivité territoriale ? *A minima*, pas moins de dix-sept ! Or, aujourd'hui, avec de simples outils disponibles sur internet, on peut aisément remonter jusqu'à sept niveaux de formatage successifs. On ne peut donc qu'être dubitatif sur la confidentialité des fichiers supprimés... "Vidanger" réellement un disque dur avant de l'envoyer au rebut exige donc un peu de temps et un minimum de précaution. Imaginons que les disques durs d'ordinateurs de fonctionnaires travaillant à l'Etat-civil ou à la direction financière d'une collectivité territoriale tombent ainsi entre les mains de personnages malveillants….

Regardons maintenant du côté du droit. Le droit des TIC en France est essentiellement d'origine jurisprudentielle, même s'il existe évidemment un certain nombre de lois relatives à la sécurité numérique. Toutefois, les magistrats n'étant pas spécialistes, corrélé au fait que l'informatique progresse en permanence, il leur faut néanmoins trancher les cas réels qui se présentent à eux. A cet égard, on ne peut que se réjouir de voir se mettre en place, peu à peu, un axe fort dans le domaine du droit relatif à la cybersécurité. Confronté à des cas complexes, le juge va mandater le plus souvent un expert en lui posant diverses questions, mais surtout une, essentielle : à la date précise où a été commise l'infraction, les précautions nécessaires et suffisantes avaient-elles été prises – eu égard à l'état de l'art au moment considéré – en matière de sécurisation des données ? S'ensuit dès lors une réponse binaire : oui ou non. Dans le premier cas de figure, le dirigeant n'a rien à craindre. Dans le cas contraire, il est susceptible d'être mis en cause. Car il n'y a pas en la matière de délégation de pouvoir en matière de protection de données à caractère personnel. Cela est valable pour l'entreprise comme pour les collectivités, jusqu'au président de la collectivité.

Il est navrant de constater que dans la plupart des organisations, on a beau répéter qu'il est impératif de prendre les mesures les plus élémentaires, on a le plus souvent l'impression de prêcher dans le vide.

Parallèlement à cela, l'âge du dirigeant constitue un paramètre essentiel. On observe le plus souvent que, plus le dirigeant est âgé, plus il est réticent à aborder les questions de risques numériques. Et ce phénomène se retrouve dans les organisations tant publiques que privées. De plus, dans le secteur privé, le critère essentiel qui va déterminer l'attaque contre une entreprise n'est plus sa taille ou son secteur d'activité mais sa capacité d'innovation. Ainsi, une entreprise de quelques dizaines de personnes, mais très innovante pourra constituer – le plus souvent à l'insu de ses dirigeants – une cible de choix dans la guerre économique actuelle. Il s'agit là d'un paramètre qu'il est difficile de faire admettre aux managers français. Or c'est là pour l'entreprise une question de vie ou de mort. Dans ma carrière au sein de la gendarmerie, j'ai ainsi vu nombre de petites sociétés se faire "hackées" et même pillées de fond en comble, pour finalement être conduites à la faillite. Il est navrant de constater que dans la plupart des organisations, on a beau répéter qu'il est impératif de prendre les mesures les plus élémentaires – ne pas se déplacer avec son ordinateur, préférer des clés cryptées, etc. – on a le plus souvent l'impression de prêcher dans le vide ! Ce n'est qu'après avoir connu une attaque numérique que la direction générale de l'entreprise va se décider à changer ses (mauvaises) habitudes.

A quelles mutations les collectivités territoriales sont-elles confrontées en ce domaine ?

Elles doivent aujourd'hui faire face à quatre défis majeurs. Le premier réside en la maitrise de leur image sur internet et sur les réseaux sociaux. Cet aspect est maintenant à peu près correctement apprécié et pris en compte. Le second, c'est leur capacité à remplir les missions de la "e-administration". Le troisième, c'est leur aptitude à faire vivre la "e-démocratie". Enfin le quatrième porte sur la dématérialisation des appels d'offre. Quand on connaît la réalité des faits, on s'aperçoit que les collectivités locales françaises sont loin d'être au point en matière de sécurisation de ces différentes missions. Si on garde à l'esprit que 60% d'entre elles comptent moins de 2.000 habitants, on mesure alors l'ampleur du travail qui reste à accomplir ! Ces petites collectivités n'ont pas, intrinsèquement, les moyens de mettre en place une vraie politique de sécurité des systèmes d'information. Il s'avère donc indispensable de passer à l'échelon administratif supérieur, à savoir l'Établissement public et coopération intercommunale (EPCI). De plus en plus, la mutualisation se révèle être un impératif.

Prenons un exemple simple et anodin en matière de e-administration : réserver une place pour ses enfants dans un club de loisirs de sa commune. Pour cela, il s'avère nécessaire de remplir en ligne des formulaires qui contiennent nombre de données personnelles. A ces flux de données succèdent des

flux financiers, qui induisent le calcul du quotient familial afin de moduler le tarif final de la prestation. D'où l'impérieuse nécessité de sécuriser ces flux, car il existe clairement un risque de piratage à des fins criminelles ou frauduleuses.
Autre exemple : après chaque délibération, le conseil municipal est tenu de l'envoyer au service préfectoral *ad hoc* pour assurer ce qu'il est convenu d'appeler le "contrôle de légalité". Là aussi, il est impératif que les flux soient sécurisés. De même si vous souhaitez conduire une enquête publique ou un référendum sur le territoire communal : les administrés internautes vont devoir donner leur avis par retour de mail. Or, ces derniers ne souhaitent pas forcément que leur opinion politique ou sociétale se retrouve sur Internet.
Autre point, encore plus problématique, car concernant des enjeux économiques majeurs : la dématérialisation des appels d'offre. Elle est certes de nature à réduire les coûts humains et matériels de traitement. Ainsi, elle offre de nouvelles perspectives à des PME qui rechignaient naguère à passer sous les fourches caudines du Bulletin officiel d'annonces des marchés publics (BOAMP) du fait de la lourdeur des procédures administratives. Mais *quid* de la fraude induite par des hackers qui n'auront aucun mal à pénétrer les serveurs non-sécurisés des mairies ? Plus besoin de complicités internes pour être informé de la stratégie du concurrent. Pas vu, pas pris ! Tels sont les défis actuels - sans parler du futur - auxquels sont confrontées les collectivités locales.

L'intérêt croissant pour l'*open data* complique-t-il la donne ?

Oui, indéniablement. Mettre à disposition des données est une bonne chose en soi, à condition toutefois de rendre véritablement anonymes ces données en amont. Sachant qu'un anonymat partiel est de nature à être contourné en usant de méthodes de recoupement indirectes, en croisant des données. Il convient par conséquent d'être extrêmement prudent quant à la nature des données que l'on va ainsi rendre publiques. De même, le cas des objets connectés doit appeler à la vigilance, sachant qu'actuellement, la plupart utilise les ressources du *low blue tooth* qui est aisément piratable. Plus généralement, je dirais qu'en France, le patron de PME ou le président d'un exécutif local vont souvent faire montre d'une fâcheuse tendance à pratiquer la politique de l'autruche quand le réel les dérange : "*ce que je ne vois pas n'existe pas*"...
Or, nous devons bien être conscients que les criminels et délinquants font à peu près ce qu'ils veulent en matière de *social engineering* (technique d'acquisition déloyale ou frauduleuse d'information ou d'escroquerie). Malgré cela, la sécurité numérique apparaît aux gestionnaires et aux décideurs uniquement comme un poste de coût. À leur décharge, il est très difficile de calculer le ROI (Retour sur investissement) d'une politique de sécurité informatique. On évolue là dans une logique assurantielle : tant que l'on n'a pas rencontré un problème, on se demande le plus souvent quel est l'intérêt de payer… Le refus de prendre en compte le réel et d'anticiper les problèmes pour se réfugier dans une vision strictement comptable est malheureusement un travers très français.

Nous devons bien être conscients que les criminels et délinquants font à peu près ce qu'ils veulent en matière de social engineering.

Comment évaluez-vous le risque (intensité et nature), tant pour les entreprises que le tissu économique, lié à l'insuffisance des politiques de cybersécurité des collectivités ?

Avant tout, en parlant de risques, il me semble indispensable de rappeler que la base de l'électronique, réside en la capacité à faire varier un signal. On a transformé ce signal d'analogique en numérique [0 ou 1]. Ce qui signifie que – même si cela prend du temps – à peu près tout peut être décrypté. Autrement dit, la sécurité absolue en matière de systèmes d'informations n'existe pas. La seule protection – relative – réside dans le cryptage. Il est abordable pour n'importe quelle structure. Il suffit par exemple de se rendre sur le site de l'Agence nationale de sécurité des systèmes d'information (ANSSI, www.ssi.gouv.fr) qui propose des systèmes de cryptage destinés tant aux professions libérales qu'aux TPE ou PME. Gardons aussi à l'esprit que les quatre postes les plus susceptibles d'être piratés dans une entreprise sont le Directeur Général, le DAF, le Directeur commercial et le directeur R&D.
Comme nous l'avons vu, le risque majeur réside dans les piratages liés aux vols d'informations stratégiques. Parlons clairement : les entreprises doivent se protéger elles-mêmes dans la mesure où elles ne peuvent tout attendre de l'État et encore moins des collectivités territoriales. Mon expérience personnelle (plusieurs centaines de conférences réalisées devant des décideurs publics et privés) m'amène à penser que, tant que l'on n'a pas évoqué des exemples frappants concernant directement les entreprises, les dirigeants ont tendance à voir ces problèmes de loin, estimant le plus souvent que leur organisation n'est pas de nature à constituer une cible : c'est le principe du "*qui voulez-vous que mes données intéressent ?*". Or, rien n'est moins vrai et c'est la raison pour laquelle il convient de mener une communication très ciblée dans le domaine de la cybersécurité, en plaçant les décideurs – présidents d'exécutifs locaux ou chefs d'entreprises – face à leurs responsabilités, notamment légales, en ce domaine. Pour prendre dès à présent cette problématique à la racine, il me paraîtrait opportun de faire des cours de sensibilisation aux nouvelles

La sécurité absolue en matière de systèmes d'informations n'existe pas. La seule protection - relative - réside dans le cryptage.

menaces, à l'intelligence économique et aux risques numériques à tous les étudiants, qu'ils soient en écoles de management, en écoles d'ingénieurs ou à l'université. Car quel que puisse être plus tard leur domaine d'activité, ils seront inéluctablement confrontés à ces nouveaux défis. Un simple ensemble d'une dizaine d'heures de sensibilisation leur permettrait d'intégrer ce paramètre dans leur "disque dur personnel" et de rester l'esprit en éveil. Des élèves du supérieur avisés seront demain des cadres prudents, en tout cas plus prudents que leurs prédécesseurs….

Rémy Février et Jean-Guy Bernard : l'aporie majeure en matière de cybersécurité réside en la prise de conscience du réel. Finissons-en avec la politique de l'autruche !

Quid de la situation des collectivités locales françaises au regard de ce que l'on observe dans d'autres pays ? Et quelles sont les pistes que vous recommandez pour une prise de conscience en France ?

On a, en réalité, peu de visibilité sur ce qui se passe réellement à l'international. Il est déjà difficile d'avoir des données fiables en France, aussi serait-il présomptueux de prétendre savoir ce qui se passe à l'étranger... En réalité, ici comme ailleurs, c'est bien plus une question de mentalité que de simple savoir-faire technique proprement dit. Même si l'on évolue dans une sphère qui apparaît comme éminemment technologique, on en revient toujours à un aspect humain, à savoir la prise de conscience du réel et la capacité à agir en fonction de cette perception. Au cours de mes interventions, je rappelle toujours que le risque majeur réside avant tout entre le clavier et la chaise. Le meilleur exemple en est une personne qui, disposant de tous les boucliers techniques nécessaires sur son ordinateur, passerait néanmoins son temps à s'exposer sans précaution aucune sur les réseaux sociaux…

Extrait portant sur le rôle de l'Etat (*Les Collectivités Territoriales face aux menaces numériques*, in *Gestion et management public*, 2013/1, Vol. 1/n°3) : *"Le manque de moyens structurels des collectivités les plus modestes, associée à l'absence de prise de conscience par les dirigeants territoriaux de l'ampleur de l'effort à accomplir afin de sécuriser les informations qui transitent par leur SI, rend d'autant plus indispensable le recours à l'État, seul à même de définir et de mettre en place une politique publique de sécurisation des SI des collectivités territoriales."*

Pour en savoir plus : *Les collectivités territoriales face à la Cybercriminalité,* par Rémy Février, éditions ESKA, 2014

Abstract

How can territory communities and their ecosystems face the threat of new digital risks?

Dr Rémy Février, an expert in Economic Intelligence and Information Systems Security, is one of the finest experts in Cyber Security in France. As an Associate Professor at EM Normandie and a Senior Lecturer at the *Conservatoire national des arts et métiers* (CNAM), Rémy Février, a former Senior Officer of the *Gendarmerie Nationale*, spells here some of the lessons drawn from his experience, both in business organisations, State Services and Territory Authorities.

In this interview with EM Normandie's Director General, Jean-Guy Bernard, Rémy Février underlines the major risks that territory communities in particular face in their relationships with their social and economic environments. Beyond straightforward technical specifics, he stresses the importance of a true realisation of this at all levels of responsibility, whether elected officials, civil servants or other decision makers. Digital risks are relentlessly on the rise. To overlook this fact is to lay oneself open to be plundered, and thus lose in the economic warfare.

Comprendre & Entreprendre
Une publication de l'EM Normandie
Directeur de publication : Jean-Guy Bernard
Illustration Rossana - ISSN en cours

Contact : Ludovic Jeanne - IDéT
EM Normandie 9, rue Claude Bloch 14052 Caen cedex 4
Tél. : +33 (0) 2 31 46 78 87
Courriel : idet@em-normandie.fr - www.em-normandie.fr

Notre vision de l'Intelligence Économique et Territoriale

Comment rétablir dans nos économies le sens du stratégique, réhabiliter le long terme, se protéger tout en se montrant innovant ? En conciliant veille et action, vision et pragmatisme, l'Intelligence Économique & Territoriale (IE&T) s'impose comme un levier de compétitivité. Ensemble cohérent de pratiques et de connaissances, l'IE&T aide les entreprises comme les territoires à se positionner, se défendre mais aussi anticiper et se développer. Agir avec succès exige d'éclairer l'action par une compréhension fine des marchés et des environnements. À cet égard, l'IE&T est l'affaire de tous. Car le sens des responsabilités de chacun décide du succès commun.

De fait, l'IE&T s'impose à la fois comme un mode d'action et un regard multidimensionnel, cherchant à comprendre la complexité du monde pour mieux la maîtriser. L'IE&T nous invite ainsi à redéfinir nos cultures organisationnelles, à revoir nos pratiques et nos méthodes. Rien ne se fera sans convergence entre acteurs publics et privés, sans l'adhésion de tous à un projet commun, enraciné dans un territoire. Face aux nouveaux défis, mêlant harmonieusement action et réflexion, l'IE&T constitue le socle des succès à venir.