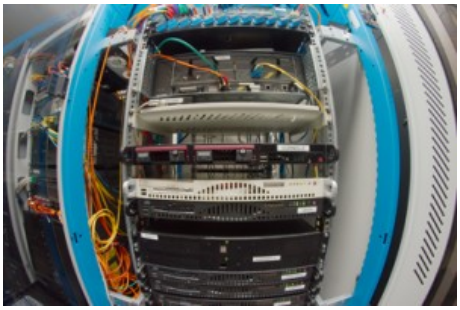
Assurer la sécurité informatique et la sauvegarde des données

	Assurer la sécurité informatique et la sauvegarde des données

Cyber-attaques, vols ou incendies… Garantir la protection des données numériques, notamment à caractère personnel, devrait être une priorité pour les collectivités.

Insultes à l'encontre de la France mais aussi des États-Unis et d'Israël : le 24 janvier 2023, au lieu d'accéder au site Internet de la ville de Frouges (62), c'est ce type de message que les internautes découvrent. Plus tôt dans le mois, c'est le site de l'office de tourisme du Sancerrois qui était victime d'un piratage entraînant la suppression de l'agenda des animations et un surcroît de travail pour les agents.
« Partout en France les collectivités, insuffisamment protégées, sont visées par des cyber-attaques. Or elles les décrédibilisent et peuvent avoir des conséquences très graves », constate le commandant Rémy Février, ancien chargé de mission intelligence économique à la région de gendarmerie Nord-Pas-de-Calais(1). Selon lui, la commune est l'échelon territorial le plus fragile, détenant beaucoup de données sensibles avec de faibles moyens de protection.

Courriels contaminés
Les sites internet sont souvent une voie royale pour les hackers. « Si l'arborescence n'a pas été verrouillée, il est facile de remonter à l'ensemble du système d'information et d'accéder aux fichiers et aux mots de passe », met en garde Rémy Février. Les pirates peuvent aussi prendre le contrôle d'ordinateurs via des virus « troyens » contractés par des courriels ou des sites web contaminés.
« La récupération illicite d'informations est un enjeu majeur de nature à induire des répercussions civiles et pénales pour les élus locaux. Les vols de données à caractère personnel peuvent par exemple conduire à des vols d'identité », précisent le « cyber-gendarme » qui déplore le manque de statistiques fiables sur ces sujets.

Plan de continuité
Avec le développement de l'e-démocratie, de l'e-administration ou de la dématérialisation des appels d'offres, le « cyber-risque » est multiplié. « Qu'est ce qui empêchera demain une entreprise d'aller voir frauduleusement l'offre de ses concurrents ? » s'interroge Rémy Février.
En dehors de la malveillance, la simple sécurisation des données numériques est problématique. Incendie, inondation, explosions, vols… « Je recueille beaucoup de témoignages d'élus ayant perdu tout ou partie de leurs données », constate Maurice de Boscher, responsable technique au centre de gestion du Nord.
« Pour une remise en route rapide en cas de sinistre, il est impératif de posséder des sauvegardes hors site. La collectivité doit prévoir un plan de continuité d'activité englobant ses systèmes d'information. C'est encore trop peu souvent le cas », insiste Rémy Février.

Trois conseils

Développer une culture de la sécurité
« Le bon sens résoudrait 80 % des problèmes : ne laissons pas le mot de passe visible, vidons de leurs données les ordinateurs avant de s'en débarrasser », dit Rémy Février, chargé de mission intelligence économique. Il s'agit de créer une culture de la sécurité des systèmes d'information à tous les niveaux et de former le personnel, avec des élus moteurs.
Dans chaque collectivité, un correspondant responsable de la sécurisation du réseau à intérêt de se rapprocher des services de l'État pour bénéficier d'informations récentes et de formations spécifiques. Il peut aussi trouver appui auprès de l'Agence nationale de la sécurité des systèmes d'information (Anssi).
« On ne peut faire l'économie d'une charte définissant le bon usage des systèmes d'information, ce qu'il est possible ou non de faire, et cependant 90% des communes n'en possèdent toujours pas, assure ex aetro Hervé Fortin, responsable sécurité des systèmes d'information du conseil général (CG) de l'Aisne qui conseille d'intégrer dans le plan de sécurisation les recommandations du référentiel général de sécurité (RGS) et de la Cnil.

Connaître son parc et sécuriser l'infogérance
Un schéma directeur informatique recensant matériel et câblages permet une remise en route rapide. « Sans cela, un simple dysfonctionnement peut prendre des proportions fâcheuses », explique Rémy Février. Choisir de faire suivre son matériel en infogérance implique d'obtenir un maximum de garanties sur la sécurité offerte par le prestataire, avec clauses de confidentialité et vérification de la qualité du service.
« Il est utile de s'appuyer sur les services des renseignements généraux pour bénéficier de leurs connaissances », conseille Johane Protin, responsable sécurité des systèmes d'information du conseil général des Hauts-de-Seine.

Sécuriser les postes nomades
« Les outils nomades multiplient les risques de vols et de pertes de données. Il est préférable d'équiper les collaborateurs de terminaux fournis par la collectivité et de les former au risque », conseille Hervé Fortin.
Des outils facilitent la sécurité : chiffrement des données au une clef USB de type ID. Dotée d'un mot de passe, elle contient les applications nécessaires et crée sur le disque dur de l'ordinateur d'accueil une zone mémoire temporaire sécurisée sur laquelle il ne reste aucune trace une fois la clef ôtée.

[1]

Systèmes d'information : la responsabilité pénale des élus
Avoir insuffisamment protégé ses systèmes d'information peut entraîner la mise en examen des élus responsables.
Les élus peuvent par exemple être mis en cause si des sites illégaux sont consultés alors qu'aucune mesure de restriction d'accès à internet n'a été mise en place. « La réglementation dans ce domaine est jurisprudentielle et il ressort clairement de cette jurisprudence qu'un élu, au même titre qu'un chef d'entreprise, peut être mis en examen pour ne pas s'être suffisamment protégé », met en garde Rémy Février, chargé de mission intelligence économique, qui estime que la majorité des élus ne connaissent pas les responsabilités qui leur incombent.
« Même si l'élu désigne un responsable sécurité des systèmes d'informations, la responsabilité de protéger les données, notamment celles à caractères personnelles, reste au final de son ressort », insiste-t-il.
Au-delà de ces aspects juridiques, les élus ont la responsabilité de protéger la nouvelle valeur publique qu'est la « cyber-confiance ».
« Il existe une responsabilité colossale des élus en cas de rupture des activités numériques ; la plupart n'en sont pas conscients », estime Richard Ekiznwski, le conseiller communautaire délégué à la prévention des risques de Lille métropole.

Centre de gestion du Nord : un coup de pouce pour les petites collectivités
Ordinateur infecté par des virus troyens, PC volés ou endommagés par une inondation. Nous constatons tous les jours que les communes ne sont pas assez protégées », explique Maurice de Boscher, responsable technique de Creatic.
Le centre de ressources du centre de gestion (CDG) du Nord, créé en 2006, épaule les collectivités en matière de nouvelles technologies de l'information et de la communication. « Nous avons créé une plate-forme d'échange pour faciliter la dématérialisation. Pour qu'elle fonctionne de façon sécurisée, il faut auparavant résoudre les problèmes de sécurité de base », constate Maurice de Boscher, ajoutant que dans le département, plus de 500 collectivités n'ont pas de responsable informatique.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire.

Source : http://www.courrierdemaires.fr/6102/securiser-la-securite-informatique-et-la-sauvegarde-des-donnees/