Colonel Laurent VIDAL – CREOGN – 30/11/2016

L'Homme, maillon faible de la chaîne SSI ?

La problématique de la négligence humaine et ses conséquences sur les collectivités territoriales.

Colloque « la transformation numérique pour les collectivités territoriales : quels enjeux de sécurité et quels accompagnements ? »

Vannes - 1er décembre 2016

Introduction :

La sécurité informatique est désormais l'affaire de tous, car le numérique s'est infiltré dans toutes les sphères de nos existences. La vie privée, le travail, les loisirs sont largement liés aux outils numériques. Les collectivités territoriales ne sont pas en dehors de cette problématique. Elles collectent, produisent et diffusent de la donnée, souvent liée à des informations personnelles ayant trait à l'intimité des personnes. Depuis la vie des enfants (état-civil, cantine, sports, école…) jusqu'au décès des proches, tout ou presque a des applications numériques. Considérer que l'administration, qu'elle soit locale, départementale, régionale ou nationale, est à l'abri des hackers est une erreur grossière. Considérer que le système est tellement sécurisé qu'il n'est qu'optionnel de se conformer à des bonnes pratiques est une erreur au moins aussi grave. Comme dans toute chaîne, c'est le maillon de la sécurité informatique le plus faible qui fixe le degré de résistance de l'ensemble. Quand les responsables SSI font bien leur travail et que les outils techniques sont efficaces, le maillon faible, c'est l'Homme...

I. Enjeux

Les communes et les collectivités territoriales hébergent ou ont accès à de nombreuses bases de données :

- état-civil
- cadastre
- social (aides diverses notamment)
- médical (Établissements d'hébergement pour personnes âgées dépendantes, centres de soins...)
- culturel (bibliothèques, médiathèques, cinémas municipaux)
- sportives (clubs…)
- transports (ramassage scolaire, lignes de bus traditionnelles…)
- fiscal (marchés publics, ventes foncières…).

Tous les types de collectivités sont concernés, qu'il s'agisse des communes, des établissements publics rattachés, des établissements publics de coopération intercommunale (EPCI : communautés de communes, communautés d'agglomérations, communautés urbaines, métropoles), les départements ou les régions.

Autant de données qui sont potentiellement monnayables, soit en tant que telles (marchés publics) soit par un biais (rançon au chiffrement, menace de dénaturation des données…).

C'est en quelque sorte toute la vie des Français qui est ainsi stockée sous forme numérique, avec des conséquences directes sur le quotidien des personnes en cas de difficultés pour les exploiter ou les actualiser. Les collectivités territoriales ont donc la main sur ce que l'on pourrait appeler des données d'intérêt général. L'idée de service public de la donnée n'est pas très loin… La loi 2016-65 du 16 octobre 2016 pour une République numérique oblige d'ailleurs les concessionnaires d'un service public informatique délégué à fournir en format ouvert librement accessible l'ensemble des données collectées ou produites pendant l'exploitation du système.

Les services publics doivent protéger les données qu'ils collectent et traitent, donc prendre les mesures techniques nécessaires pour parvenir au niveau de protection souhaité. Les données médicales font l'objet d'un traitement particulier en matière de sécurité, les hébergeurs devant être agréés après vérification des systèmes de protection mis en place. L'exigence de protection est d'autant plus élevée que les obligations prévues par le règlement UE du Parlement et du Conseil du 27 avril 2016 (entrant en vigueur le 27 mai 2018) sont contraignantes et lourdement sanctionnées.

II. Cybermenaces

L'individu peut être le maillon faible de la chaîne de sécurité des systèmes d'information. Pour contourner les moyens de défense informatique, rien de tel, en effet, que de se servir d'une personne qui a légitimement accès au réseau et aux bases de données qui y sont connectées. Ce phénomène est universel : lorsque la sécurité des voiture s'est durcie, les voleurs se sont attaqués aux conducteurs, pour voler les clefs. Dans le cas des réseaux, la violence n'est pas nécessaire. Il suffit de trouver un point d'entrée et de s'y engouffrer.

Ce point d'entrée peut être trouvé par le forçage informatique des sécurités (mais ce procédé est potentiellement complexe et peut déclencher des alertes), par une intrusion dans les locaux (mode d'action encore plus risqué puisqu'il suppose une présence physique) ou par un accès réalisé par une personne habilitée. Dès lors se pose la question du moyen à utiliser pour obtenir d'un complice la réalisation des manipulations souhaitées.

Pour avoir un « pied dans la maison », il est possible de faire appel à un complice. Ce peut être un employé mécontent ou une personne travaillant chez un sous traitant par exemple. Il est aussi possible de forcer la main à une personne choisie pour sa capacité à accéder, depuis son poste de travail, à l'infrastructure informatique visée. Le chantage est dans ce cas un mode de pression possible. Enfin, le hacker pourra compter sur l'imprudence ou la naïveté pour implanter son logiciel malveillant dans le système dont il souhaite percer les défenses.

En juillet 2015, un groupe de hackers a piraté le serveur d'un site spécialisé[1] qui permettait d'organiser des rencontres extraconjugales en promettant par ailleurs la plus grande sécurité pour les données hébergées. Ce groupe a aspiré les données (messages, adresses de messagerie…) concernant près de 35 millions d'utilisateurs sur les 40 millions revendiqués par le site. Il a ensuite adressé une mise en demeure aux gestionnaires du site demandant sa fermeture puis, sans réponse de ces derniers, a mis en ligne près de 20 Go de données. Cette chasse aux « infidèles immoraux » ne prête cependant pas à rire. Des internautes n'ont pas tardé à recevoir des mails de maîtres chanteurs menaçant de révéler à leur conjoint leur présence bien inconfortable dans la liste des clients du site… Cette situation permet de se faire verser de l'argent (en Bitcoin pour plus d'anonymat…) mais peut très bien être utilisée pour obtenir un service particulier comme par exemple le fait de dévoiler ses codes d'accès à un serveur ou d'insérer une clé USB chargée d'un malware dans un ordinateur.

En février 2000, en Australien, un employé d'une station de traitement des eaux mécontent de ne pas bénéficier d'un avancement de la part des autorités du comté a piraté les serveurs informatiques qui pilotent la station. Avec des instructions passées par informatique, il a fait ouvrir les vannes de bassins de rétention et provoqué la pollution à grande échelle de la rivière Maroochy.

L'attaque pourra prendre la forme d'une clef USB laissée négligemment par terre sur le trajet d'une personne employée dans a collectivité visée. Si cette clef porte en plus le logo de cette collectivité, il est possible que la personne qui la ramasse la branche sur le lecteur de son ordinateur de bureau pour essayer d'en identifier le propriétaire et lui pouvoir lui rendre (c'est tellement embêtant de perdre ses données avec une clef…). Sauf que la clef porte en elle un virus qui va infecter le système et pourra provoquer, selon les objectifs poursuivis, une prise de contrôle à distance, un chiffrement des données en vue d'une rançon ou encore la destruction des données. En février 2016, un hôpital américain a fait les frais d'un tel scénario[2]. Le *Hollywood Medical Prebyterian Center* a dû verser 17000 dollars pour pouvoir accéder à nouveau à ses données qui avaient été mises hors d'atteinte par un chiffrement. Le service administratif s'est retrouvé momentanément bloqué, empêchant l'admission de nouveaux patients.

1 http://www.01net.com/actualites/ashley-madison-le-hack-qui-expose-les-phantasmes-de-37-millions-d-individus-adulteres-908424.html
http://www.lesinrocks.com/2015/08/20/actualite/pourquoi-il-ne-faut-pas-rire-du-hack-dashley-madison-11768231/

2 http://www.zdnet.fr/actualites/quand-un-ransomware-paralyse-un-hopital-americain-39832906.htm

III. Quelles réponses face à ces menaces ?

1. Architecture du réseau / droits des utilisateurs

L'architecture du réseau doit permettre de protéger les données. L'accès à certains services peut ainsi être subordonné à la fonction de l'utilisateur. Dans la gendarmerie nationale, les personnels civils et militaires sont placés dans un organigramme qui prend en compte leurs fonctions et génère de façon automatique des droits d'accès à certaines parties de l'Intranet ou aux fichiers centraux. Ainsi, un commandant de groupement peut, pendant son temps de commandement, accéder en tant qu'OPJ à l'ensemble des fichiers judiciaires et administratifs disponibles sur Intranet. Cette faculté cesse d'elle-même après son départ du groupement pour un poste en administration centrale. De la même manière, un gendarme adjoint APJ n'a pas les mêmes accès qu'un sous-officier OPJ ou qu'un civil servant au sein d'un groupe de commandement. Cette politique de gestion des droits d'accès permet d'une part de limiter les risques d'accès non autorisé à certains fichiers particuliers (limitation stricte au droit à en connaître) et d'autre part de contrôler les accès et les consultations sur certains sites et fichiers. Cette politique nécessite une identification forte des utilisateurs. Dans le cas de la gendarmerie nationale, cette identification, après avoir longtemps reposé sur le seul binôme identifiant / mot de passe, est validée, pour l'accès à certaines fonctionnalités, par l'utilisation de la carte professionnelle. Insérée dans un lecteur, cette dernière est elle aussi renforcée par l'usage d'un code PIN. Notons que le système informatique oblige les utilisateurs à changer le mot de passe tous les six mois et empêche même la réutilisation d'un mot de passe ancien.

Les serveurs doivent bien évidemment être protégés par des pare-feu et faire l'objet de sauvegardes journalières. Ces sauvegardes constituent une sécurité en cas de défaillance du matériel principal, toujours possible, mais aussi lorsque les données du serveur habituel se trouvent contaminées ou dénaturées. Les branchements sur le réseau doivent être faits uniquement avec des ordinateurs mis en place par le service SIC, configurés et conformes à la politique de sécurité informatique de l'administration concernée. Le SSI doit également disposer d'une cartographie précise du système. Cette cartographie doit être tenue à jour et enrichie en permanence en fonction des nouveaux matériels utilisés et des évolutions logicielles. La liste des logiciels dont la présence sur les ordinateurs du réseau est autorisée fait également partie de la cartographie. Un logiciel robot pourra utilement rechercher sur les disques durs la présence de logiciels non conformes, installés par un utilisateur soucieux de son confort ou réticent à se servir d'une application imposée par l'administration…

2. Hygiène informatique

L'ANSSI met en ligne un guide d'hygiène informatique[3]. En 52 pages et 40 règles, cet opuscule balaie l'ensemble des mesures à prendre s'agissant des gestionnaires et des utilisateurs de systèmes informatiques, en se concentrant sur les systèmes bureautiques classiques.

Les recommandations sont parfois techniques mais relèvent finalement le plus souvent du bon sens. Les utilisateurs sont en fait invités à considérer que l'ensemble des moyens informatiques et numériques hors réseau sont potentiellement suspects. Les clefs USB, les disques durs portables, les cartes SD des appareils photo, les appareils connectés, les téléphones et tablettes peuvent servir de porte d'entrée pour les logiciels malveillants. Les téléphones portables, par exemple, ne doivent pas être banchés sur la prise USB du PC de bureau pour recharger la batterie : rien ne permet d'affirmer qu'une connexion non souhaitée ne s'établira pas entre le téléphone (connecté au réseau GSM) et un poste lointain, avec accès direct au disque dur du PC… D'une manière générale, les connexions sans fil sont à prendre avec précaution. Tout réseau hertzien est par nature susceptible d'être intercepté par un tiers. « Sniffer » les connexions est facile et repérer celles qui ne sont pas sécurisées l'est encore davantage. Aller faire un tour sur le site Shodan[4] est particulièrement éclairant sur ce point. L'Internet des objets est plutôt devenu l'Internet des systèmes d'objets connectés : chaque système (par exemple le système de l'individu, avec son bracelet, sa montre, son téléphone, sa tablette, son implant médical connectés) entre en connexion avec les autres, s'y insère, y évolue et échange de très nombreuses données. Ces points de connexion constituent autant de portes d'entrée qui nécessitent l'attention des responsables SSI et des mesures de sécurisation de la part de leurs propriétaires.

Mais l'hygiène informatique ne s'arrête pas aux portes de l'entreprise. Elle doit également être appliquée chez soi et dans son usage quotidien d'Internet. L'usage des réseaux sociaux notamment doit se faire avec la plus grande rigueur et sans perdre de vue que rien de se qui s'y passe ne peut être oublié ou effacé et qu'il est très facile de se compromettre ou de compromettre son entreprise. Depuis les selfies pris sur une chaîne de production industrielle (avec en arrière plan la machine dernier cri…) jusqu'aux informations sur les collègues de bureau, les fouineurs intéressés ont beaucoup à apprendre sur un individu grâce aux informations complaisamment publiées sur Facebook, Linkedin ou Twitter.

Le *social ingineering*[5], lorsqu'il est bien mené, peut permettre de bâtir un organigramme d'administration, d'identifier les responsables clefs et ensuite de décliner pour chaque profil jugé intéressant une carte d'identité bien particulière comprenant les

3 http://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
4 https://www.shodan.io
5 Mode de recherche qui croise des informations disponibles sur des réseaux sociaux, des sites Web et autres sources d'information ouvertes et permet, comme un puzzle, de reconstituer des organigrammes hiérarchiques, les liens entre personnes, les affinités communes, etc.

hobbies, les petites faiblesses ou encore les avis sur telle ou telle personne. Une fois la victime identifiée et cernée, les délinquants sauront quel levier activer pour provoquer la réaction attendue et obtenir ce qu'ils désirent (information, accès à un fichier, argent…).
Un guide des médias sociaux peut utilement être développé et distribué aux collaborateurs afin de les mettre en garde et de leur indiquer la bonne conduite à avoir.

En guise de conclusion…

Code PIN, identifiant, mot de passe sont souvent vécus comme de vrais lourdeurs. On aimerait pouvoir s'identifier par un simple regard, que la machine vous reconnaisse toute seule et qu'elle fasse d'initiative l'ensemble du travail de sécurité… Douce rêverie qui, à l'heure où ces lignes sont écrites, ne correspond pas à la réalité. Prendre des mesures de sécurité, s'assurer qu'elles sont bien appliquées, effectuer les rappels nécessaires aussi souvent qu'il le faut ne constituent pas des options. Dans le secteur public comme dans le secteur privé, il est indispensable de faire prendre conscience aux collaborateurs que la sécurité de l'ensemble passe aussi par leur comportement et aussi (surtout?) que ces mesures de prudence doivent s'élargir au périmètre de la vie numérique privée.

Les hackers malhonnêtes n'ont pas fini de faire des victimes, de créer des pertes importantes dans le secteur privé mais aussi de générer des difficultés sans fin aux victimes des vols d'identité. Avoir une bonne hygiène informatique et travailler sur des réseaux robuste constitue une première et indispensable réponse.