



TIC

# Systemes d'information : la vigilance est de mise

- Des publics internes et externes accèdent à distance à des données sensibles.
- Des organisations mettent à niveau leur politique de sécurité, sans toutefois freiner cette évolution.

**E**n 2008, en réaction à son licenciement pour insubordination, un administrateur de réseau bloquait, en activant un mot de passe exclusif, l'accès à 60 % des données de la ville de San Francisco. La liste des événements décrits dans le panorama annuel de la cybercriminalité présenté par le Club de la sécurité de l'information français (Clusif) réserve à chaque fois quelques sueurs froides aux responsables de la sécurité des systèmes d'information (SI). Développe-

ment des réseaux sociaux, essor du piratage des circuits électroniques, erreurs de routage et failles de sécurité des logiciels réseaux... Leur vigilance s'accroît au fur et à mesure que le nombre d'internautes grandit et que les moyens « nomades » de se connecter se multiplient. Parallèlement, la pression est de plus en plus forte sur l'administration territoriale pour évoluer vers des échanges électroniques dématérialisés avec les usagers et avec d'autres administrations. Ainsi le challenge est de trouver les parades pour ouvrir l'accès en toute sécurité à un système d'information jugé stratégique par 68 % des collectivités territoriales.

**Authentification unique.** « Cette pression est la même, quelle que soit la taille de la collectivité, observe Lionel Mourer, consultant sécurité chez Bull et membre du Clusif. Les budgets et les ressources à consacrer ne sont certes pas identiques dans une petite commune ou un conseil général, mais aucun ne peut se dispenser d'une analyse des risques. Aujourd'hui, l'on ne traite plus ce sujet uniquement sous un angle technique, mais on met en perspective les enjeux stratégiques et les moyens utilisés. » Selon la criticité des données à protéger, les plans d'action seront plus ou moins ambitieux. Les combinaisons de solutions seront étudiées en fonction du niveau de risque acceptable et du type d'utilisateurs concernés : personnel interne ou externe, prestataires, élus, citoyens...

## LES CHIFFRES CLÉS

- 30 % des collectivités ont formalisé une politique de sécurité de l'information.
- 42 % interdisent la connexion des appareils mobiles même sous contrôle (contre 13 % dans le secteur privé).
- 95 % ont installé des antivirus, 82 % des antispham, 87 % des pare-feu, mais seuls 40 % utilisent l'authentification forte par certificat.
- 69 % sont en conformité totale avec la loi « informatique et libertés » (64 % dans le secteur privé).
- 42 % ont réalisé une analyse globale ou partielle des risques liés à la sécurité du SI.

Source : 2008 « Menaces informatiques et pratiques de sécurité en France », Clusif.

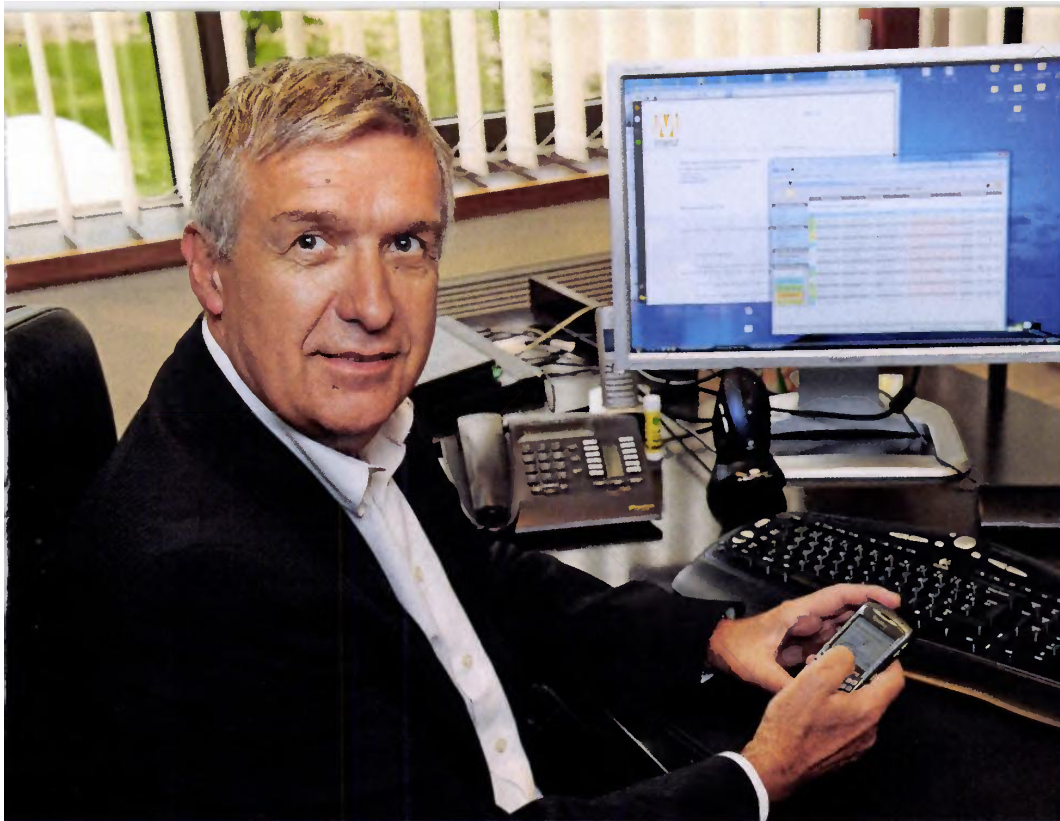
**TÉMOIGNAGE** François Fouillet, DSI de la communauté de communes Parthenay (Deux-Sèvres)

## « Un sas de sécurité entre notre site et les citoyens »

« Nous expérimentons la plateforme [mon.service-public.fr](http://mon.service-public.fr) [\*] pour offrir aux Parthenaisiens un accès cohérent aux téléservices locaux et nationaux. Nous bénéficions ainsi d'une plateforme nationale puissante qui garantit la sécurité des transactions grâce à un ensemble de mécanismes, comme la fédération d'identité. Le citoyen dispose d'un compte unique et d'un mot de passe, il bénéficie d'un espace dédié, autrement dit un coffre-fort électronique où il stocke tous ses documents scannés ou sous format électronique. Ce sas entre la mairie et le citoyen résout un certain nombre de points de sécurité qui impliqueraient une organisation et des investissements financiers au-dessus de nos moyens. Nous pouvons nous consacrer au suivi de nos téléprocédures, à l'organisation interne des informations transversales et rester vigilants au respect de la loi "informatique et libertés". »

[\*] Plateforme financée par la Caisse des dépôts et consignations, projet mené avec la Direction générale de la modernisation de l'Etat. [www.modernisation.gouv.fr](http://www.modernisation.gouv.fr)

Le b.a.-ba de la sécurité commence par les informaticiens... Par exemple, la ville de Beauvais (Oise) a profité de la refonte de son SI pour installer un annuaire de gestion et de contrôle des accès au réseau (Wallix Admin Bastion, basé sur des logiciels libres). « Ma hantise est d'avoir quatre-vingts points de connexion par lesquels l'on peut accéder à nos ressources informatiques », confie Frédéric Dupuy, directeur des SI. Un enjeu d'autant plus fort que l'équipe informatique de la ville n'est composée que de trois personnes pour gérer quarante serveurs auxquels accèdent à distance les prestataires extérieurs qui administrent le réseau. Le système mis en place identifie les personnes autorisées, supervise le réseau et conserve la trace de toutes les opérations réalisées au



### ► Circulation des données

La ville de Metz a rendu son parapheur électronique désormais accessible aux ordinateurs de poche et téléphones « intelligents » donnés aux élus et cadres dirigeants. Les aspects sécurité sont assurés par le système de cryptage du concepteur. La signature transite par internet via un site sécurisé par un réseau virtuel et des certificats SSL. « Ce dispositif de sécurité est suffisant compte tenu du caractère administratif du courrier qui y circule », assure Bertrand Lang, directeur des technologies de l'information et de la communication.

A. BERNANT

quotidien. Un seul identifiant et un mot de passe donnent accès à un certain nombre d'applications selon la nature du travail de chacun. Le système agit comme une zone tampon avec l'extérieur.

« L'enregistrement de l'activité de chacun nécessite un accompagnement de l'installation de ce genre de dispositifs. Il faut montrer les avantages en termes de partage des connaissances, en particulier pour analyser la nature des incidents, reconnaît Frédéric Dupuy. Et aussi expliquer que cela devient obligatoire dans certaines applications de dématérialisation comme les factures. » Dans ce cas, la traçabilité des opérations a aussi un impact sur la fiabilité d'un système qui doit être disponible 24 heures sur 24, en particulier pour les serveurs qui gèrent les caméras de vidéosurveillance.

**Outils nomades... prudence.** La sensibilisation aux risques est la clé de la réussite des démarches de sécurité, d'autant plus en cas de déplacements. La direction des SI doit alors établir des règles strictes pour concilier la sécurité et le désir de dis-

## Un recueil de bonnes pratiques

Le référentiel général de sécurité (RGS) recense les bonnes pratiques en la matière pour les systèmes d'information (SI). Il propose une démarche globale d'analyse et de prise en compte de la sécurité. L'objectif est d'aider à définir un niveau de sécurité en phase avec l'état de l'art et le contexte de l'administration concernée. Le RGS propose une liste de produits et services certifiés, qui sera actualisée régulièrement pour s'adapter aux nouvelles vulnérabilités d'internet. Prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques, le décret d'application du RGS est en cours d'examen au Conseil d'Etat, pour une publication attendue au deuxième trimestre 2009. La version déjà approuvée par la Commission européenne est en ligne sur [www.referencess.modernisation.gouv.fr/rgs-securite](http://www.referencess.modernisation.gouv.fr/rgs-securite)

poser d'un bureau virtuel des élus et des cadres dirigeants.

Après avoir été sollicitée par les élus, la direction des SI du conseil général de Gironde a accepté de s'adapter au cas par cas à leurs demandes. Mais la condition sine qua non est de n'autoriser l'accès à distance que pour les matériels qu'elle achète et qu'elle équipe elle-même de logiciels. La même exigence de contrôle du matériel s'applique à Metz (Moselle), cette fois pour l'application

de parapheur électronique lancée par la ville depuis 2002. Le circuit dématérialisé des courriers et bons de commande, soumis à l'approbation des cadres dirigeants et à la signature des élus, est maintenant ouvert aux connexions à distance sur ordinateur de poche et téléphone intelligent (couplé à un assistant personnel). « Nous combinons le cryptage proposé par le concepteur de la technologie "Blackberry", à l'annuaire d'autorisation de la

mairie. Nous n'avons pas ajouté de certificats sur carte à puce ou sur clé USB, qui auraient alourdi le processus. Cette sécurité est suffisante compte tenu du caractère administratif du courrier qui y circule », précise Bertrand Lang, directeur des technologies de l'information et de la communication de la ville.

**Coffre-fort électronique.** En revanche, l'ouverture du SI à l'utilisateur repose essentiellement sur la mise en place de zones tampon sécurisées accessibles par une authentification unique, afin de protéger les données privées confidentielles dont la collectibilité est dépositaire. Les questions de sécurité font partie intégrante des projets lors de mise en ligne de téléservices.

Le conseil général du Val-d'Oise met à disposition des communes du département la plateforme « Cap Démat », qui fournit un cadre technique pour activer une quinzaine de téléservices allant du culturel au périscolaire, accessibles par internet ou sur des bornes interactives. « L'accès des usagers, basé sur le protocole sécurisé "HTTPS" qui crypte >



## La pression est de plus en forte pour évoluer vers la dématérialisation

■■■ les transactions, se fait via un identifiant et un mot de passe de huit caractères minimum, détaille Philippe Usclade, chef de projet Cap Démat. L'accès à distance par les agents et le traitement des transactions se font aussi sur le principe de l'authentification unique couplée cette fois à l'annuaire d'autorisation interne à chaque commune. » Le citoyen dispose en outre d'un espace de stockage des pièces justificatives, dit « coffre-fort électronique », dont il est seul détenteur des codes d'accès, les agents ne visualiseront donc ces documents que lors de l'instruction d'une démarche.

**Extension.** Les mêmes principes président à l'expérimentation de « mon.service-public.fr » par la communauté de communes de Parthenay (Deux-Sèvres) et Vandœuvre-lès-Nancy (Meurthe-et-Moselle), avant d'être généralisée à l'ensemble des collectivités, sous la forme d'un kit d'accès gratuit. Le concept de compte unique est étendu à tous les services locaux et nationaux. Parthenay teste, par exemple, une application « nouvel arrivant » qui permet à une famille avec enfant de s'inscrire aux services de la commune liés à l'enfance et fait le lien avec la Caisse d'allocations familiales. Ceci sans risque de recoupement de fichiers d'informations personnelles, conformément aux préconisations de la Commission nationale de l'informatique et des libertés.

Sophie Maréchal

### CONTACTS

- **Nicolas Bunoust**, responsable de la sécurité du système d'information de Loire-Atlantique, tél. : 02.40.99.11.93.
- **François Fouillet**, DSI de Parthenay, tél. : 05.49.94.90.00.
- **Bertrand Lang**, directeur des technologies de l'information et de la communication de Metz, tél. : 03.87.55.51.10.