La sécurité des systèmes d'information (SSI) en gendarmerie

Jean-Marc Texier

Colonel
responsable de la sécurité
des systèmes d'information de la Gendarmerie nationale
au ST (SI) 2

1979-1987 : service national en Gendarmerie et parcours montagne

En février 1979, j'ai débuté ma carrière dans la gendarmerie en intégrant le Centre d'instruction de gendarmes auxiliaires (CIGA) de Saint-Astier (Dordogne). La formation a duré deux mois pour les classes (formation initiale) et deux mois au peloton de gradés. À l'issue de ces formations, j'ai été affecté au peloton de gendarmerie de montagne de Savignac-les-Ormeaux (Ariège). J'ai fait beaucoup d'entraînements et de secours en montagne, de surveillance mais aussi des secours sur piste dans certaines petites stations. Les grandes stations disposaient de secouristes. Le renfort GD dans les unités de l'Ariège m'a donné le goût pour l'institution Gendarmerie.

Un gendarme auxiliaire à la fin des années 1970.

Après mon service militaire, j'ai postulé pour faire carrière en gendarmerie comme sous-officier. Je suis entré en octobre 1980 à l'école de Montluçon. Comme j'aimais la montagne et que je suis sorti très bien classé, j'ai demandé la région PACA, non pas pour la mer mais pour servir en montagne dans les Alpes. Et j'ai été affecté à la brigade de Chorges (Hautes-Alpes) où j'ai passé six années. J'y ai préparé la qualification d'officier de police judiciaire (OPJ). Sur la circonscription nous avions des renforts estivaux pour le lac de Serre-Ponçon. Dès l'obtention de mon OPJ, le commandant de compagnie me confiait la responsabilité du poste saisonnier hivernal à la station de ski de Risoul où j'avais une dizaine de gendarmes mobiles et de gendarmes auxiliaires sous mes ordres.

1987-2002 : parcours d'officier de gendarmerie et d'informaticien

En 1987, j'ai réussi le concours d'entrée à l'École des officiers de la Gendarmerie nationale. J'en suis sorti en 1990 après une scolarité de trois années. Au passage, j'y ai rencontré mon épouse qui était au secrétariat du général, commandant l'école. J'ai choisi de servir en région parisienne à l'escadron de gendarmerie mobile de Drancy. Trois beaux déplacements outre-mer (Corse, Saint-Martin et La Réunion), des cérémonies de prestige notam-

ment quand l'escadron a servi de support pour le bicentenaire de la gendarmerie en 1991 et de nombreux services de maintien de l'ordre sur Paris ont marqué cette période.

À l'escadron, je m'étais mis à la bureautique. Je possédais un des tout premiers Macintosh et j'avais établi des tableaux pour suivre le personnel notamment à l'occasion du passage d'examens. Je me suis ensuite naturellement porté volontaire pour devenir officier informaticien. J'ai suivi une scolarité de 9 mois au Conservatoire national des arts et métiers (CNAM). Affecté à l'issue au centre de programmation de la gendarmerie, d'abord comme adjoint au chef de centre puis comme chef, j'ai participé au chantier majeur de l'époque : la vérification et la modification si nécessaire des programmes informatiques pour l'échéance du passage à l'an 2000 car pour beaucoup d'entre eux la codification de l'année était sur deux chiffres et non sur quatre. Je n'ai pas terminé le travail, car à l'été 1999, j'ai été affecté comme commandant de compagnie de gendarmerie départementale au Mans.

2002-2016 : la sécurité des systèmes d'information

Trois années de compagnie passées, en 2002, la gendarmerie m'a rappelé à la sous-direction des télécommunications et de l'informatique au bureau de la conception et de la coordination en qualité de chef de la section sécurité des systèmes d'information. Je fus le second chef de cette section après Bruno Le Hir. J'ai commandé cette section de 2002 à 2006, date à laquelle j'ai été promu lieutenant-colonel et par la même occasion affecté comme adjoint au chef du BCC devenu le BSA (bureau de la sécurité et de l'architecture). J'ai occupé cette fonction pendant deux ans avant d'être nommé chargé de projets auprès du SDTI. J'ai alors piloté un projet d'écriture d'une politique de sécurité des systèmes d'information (PSSI).

Au sein de la SDTI, j'ai notamment travaillé sur plusieurs dossiers importants : la charte de reconnaissance de responsabilité, la sécurisation informatique précédent l'arrivée de saphir 3G, la sécurisation de l'accès à Internet et la PSSI de la gendarmerie. Avant de connecter au réseau de la gendarmerie les réseaux locaux des unités de gendarmerie situés hiérarchiquement en dessous du groupement, il fallait s'assurer de leur sécurité. En particulier, il fallait maîtriser les ordinateurs, système d'exploitation, briques logicielles et applications locales. Cela a nécessité tout d'abord la réalisation d'un inventaire exhaustif de l'existant. Nous avons utilisé le logiciel Ocs Inventory pour construire cet inventaire de parc. Après études de chaque système, nous avons ensuite déterminé les logiciels ou applications sûres sur le plan de la sécurité qui pouvaient être utilisés. Le reste a été désinstallé. Nous avons limité aux seuls administrateurs techniques la capacité d'installer des logiciels. Ce préalable achevé, les unités de terrain étaient connectées au réseau de la gendarmerie et bénéficiaient d'Intranet et Internet sur leurs postes de travail.

L'accès à Internet sur le poste de travail était pour nous incontournable. Cependant, on connaît les risques sur le plan de la sécurité qu'une interconnexion mal maîtrisée peut induire. Les architectes ont donc conçu et mis en œuvre une DMZ (zone démilitarisée) permettant une séparation sécurisée entre Internet et Intranet. Nous avons aussi appliqué le principe de défense en profondeur pour ne pas miser sur une seule barrière. En particulier, le poste de travail a été sécurisé : absence de droit administrateur, présence d'un antivirus, système d'exploitation à jour des correctifs. Tout un ensemble de briques de sécurité a été déployé. Pour surfer sur Internet, le poste de travail devait être à jour des bases de signature antivirale et des correctifs. À défaut, l'accès à Internet n'était pas autorisé.

Carte professionnelle et boîtier d'accès à l'Intranet gendarmerie.

Le PSSI-G inscrit au Mémorial de l'Intranet gendarmerie.

La mise en place de la charte s'inclut dans un chantier de sensibilisation de tous les utilisateurs de l'Intranet de la gendarmerie face à certains abus et surtout pour prévenir et diminuer l'impact d'attaques. Cette réglementation a été mise en œuvre en toute transparence : nous l'avons défendue devant le directeur de la Gendarmerie nationale et communiquée au Conseil de la fonction militaire de la Gendarmerie (CFMG) tout comme aux syndicats pour les personnels civils. Sept principes composaient la reconnaissance de responsabilité :

- l'internaute connaît la législation ;
- l'internaute fait un usage professionnel des équipements informatiques et des réseaux,
- l'internaute fait de la sécurité une priorité ;
- l'internaute respecte la communauté dont il fait partie ;
- l'internaute fait montre de savoir-vivre et de courtoisie ;
- l'internaute respecte la confidentialité des informations ;
- l'internaute fait preuve de vigilance sur le réseau Internet.

La première version de la reconnaissance de responsabilité a été éditée par l'imprimerie du service de traitement de l'information gendarmerie (STIG). Cet imprimé était nominatif et adressé à chaque unité. Le personnel signait sa propre reconnaissance de responsabilité et localement, les bureaux des systèmes d'information et de communication (BSIC) saisissaient dans une application la signature effective du document. Ceux qui ne voulaient pas la signer, auraient vu leur accès à l'Intranet de la gendarmerie désactivé. Autant dire, que le gendarme ne pouvait plus travailler.

Le colonel Géraud, à la SDTI, suivait de très près les refus qui étaient traités jusqu'au retrait des droits à l'accès à l'informatique. Il n'y a eu que très peu de cas et aucun cas n'est allé jusqu'à l'extrême limite. Après cette sensibilisation massive et quelques mois pendant lesquels la non-application de principe a fait l'objet de rappels, certaines dérives dangereuses notamment pour la disponibilité du réseau ont continué. Nous avons donc décidé en rapport étroit avec le service des ressources humaines et le cabinet du DGGN, qu'il fallait désormais sévir. L'Intranet de la gendarmerie est avant tout un réseau opérationnel qui ne devait pas être perturbé par des envois de mails en grand nombre sur des sujets sans lien avec le service. Après plusieurs demandes de punition, tout est rentré dans l'ordre.

La PSSI-G, publiée en 2009, est toujours au *Mémorial de la Gendarmerie*. Son élaboration a fait l'objet d'un marché d'assistance attribué à Thalès. Nous avons rencontré toutes les directions de la DGGN, certaines gendarmeries spécialisées, des représentants du commandement des écoles ainsi que des commandants de groupement GD afin de déterminer la nature des informations traitées en gendarmerie et leur niveau de protection souhaité, les éléments essentiels indispensables à l'exécution des missions de la gendarmerie, puis les événements redoutés, les objectifs de sécurité et enfin les mesures à mettre en place. Elle est en cours de mise à jour suite à la parution de la PSSI de l'État en 2014.

En 2009, j'ai rejoint la direction de la planification de la sécurité nationale (DPSN), structure rattachée au haut fonctionnaire de Défense (HFD) du ministère de l'Intérieur, en charge notamment de la politique SSI du ministère. Cette unité est devenue un peu plus tard la direction de la prospective et de la planification de la sécurité nationale (DPPSN). Cela ne changeait en rien les missions relevant de la SSI mais la fonction prospective a pris tout son sens pour la planification et la gestion des crises. En 2012, cette partie prospective a été transférée auprès du directeur général de la sécurité civile et de la gestion des crises (DGCSGC). S'en est suivie la transformation de la DPPSN en service du haut fonctionnaire de défense (SHFD), service dans lequel j'ai pris la tête du pôle SSI à l'occasion de ma promotion au grade de colonel. Outre les missions SSI, mon passage dans ce service a été essentiellement consacré à la maîtrise d'ouvrage d'un projet majeur : la carte agent ministérielle. C'est le pendant de la carte professionnelle électronique de la gendarmerie au profit de tous les autres agents du ministère. Il m'a permis d'approfondir ma connaissance du ministère et de tous ses métiers ainsi que celle d'un domaine très particulier de la sécurité : les infrastructures de gestion de clés (IGC) et les certificats numériques. Ce sont des systèmes mal connus du grand public, mais pourtant qui sont utilisés quotidiennement sur Internet, notamment pour sécuriser les flux https.

En 2015, j'ai été affecté comme responsable de la sécurité des systèmes d'information de la gendarmerie et du ST (SI) [2]. Le chef de ce service, par la réorganisation en cours, veut montrer que la sécurité des systèmes d'information est essentielle car elle doit garantir la disponibilité, l'intégrité et la confidentialité des informations et des systèmes d'information utilisés en gendarmerie.

La SSI est devenue un enjeu majeur puisque les systèmes sont indispensables à la bonne exécution des missions opérationnelles et de soutien de la gendarmerie. L'environnement évolue aussi considérablement : la gendarmerie a besoin d'échanger des informations avec un nombre de partenaires toujours croissant augmentant ainsi les risques. Les attaques et tentatives d'attaques se multiplient pour perturber le fonctionnement de la gendarmerie ou voler des informations sensibles. Pour nous, c'est donc un chantier permanent d'adaptation à la menace, à l'évolution de nos systèmes et des briques logicielles que l'on utilise pour garantir le niveau de sécurité attendu.

Brochure de sensibilisation à la sécurité des systèmes d'information destinée aux chefs d'entreprise.