Séminaire

Bordeaux

16 mai 2017 - 14 h / 17 h

académie Bordeaux

RÉGION ACADÉMIQUE
NOUVELLE-AQUITAINE

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Quelles modalités de mise en oeuvre de la politique de sécurité des systèmes d'information au sein des établissements scolaires dans le cadre de la loi d'orientation et de programmation de 2013 ?

RÉGION Nouvelle-Aquitaine

Dordogne le DÉPARTEMENT

Département des Landes

PYRENEES ATLANTIQUES LE DEPARTEMENT

Gironde LE DEPARTEMENT

LOT-ET-GARONNE Le Département

Les actes du séminaire

Contexte du séminaire

Le séminaire dédié à la mise en oeuvre de la sécurité des systémes d'information dans les établissements scolaires s'est déroulé à Bordeaux le 16 mai 2017.

Il a rassemblé les acteurs responsables du domaine dans les services de l'Education nationale et des collectivités territoriales de l'académie de Bordeaux.

Destiné à étudier les modalités pratiques d'une SSI opérationnelle, le séminaire s'est déroulé en quatre temps de présentations et d'échanges et s'est conclu sur la projection vers une chaîne de responsabilité unifiée entre l'Etat et les collectivités.

Cette rencontre a été l'occasion d'échanger autour du référentiel académique des exigences de sécurité.

Ouverture du séminaire par la DSI/RSSI de l'académie de Bordeaux

Patrick BENAZET
DSI/RSSI de l'académie

Ouverture par Patrick BENAZET, DSI et RSSI de l'académie de Bordeaux, qui fait part du plaisir non dissimulé pour l'ensemble de l'institution d'accueillir les collectivités sur cette thématique.
Il présente Dominique ALGLAVE, RSSI du ministère, venu porter la parole de l'administration centrale dans toutes ses dimensions et Jean-Louis BRUNEL, Responsable du pôle national de sécurité d'Aix Marseille ainsi que les membres de l'équipe SSI de l'académie de Bordeaux, Laure COULON et Lionel LOPEZ, Adjoints au RSSI. Ces différentes personnes œuvrant dans un cadre de dialogue partenarial.

La démarche de ce séminaire a été libellée sous la forme interrogative pour définir ensemble les conditions dans lesquelles l'exercice de la sécurité dans les EPLE va être conduite dans les prochaines années.

Patrick BENAZET insiste sur le caractère participatif du séminaire dans le but d'aboutir à des choses faisables, des principes soutenables, des modalités de financement réalistes. Les modalités de mise en œuvre de la politique de sécurité des SI des EPLE doivent être connues, donc avoir une existence avant tout.

L'objectif est de rédiger un document qui sera signé par le recteur et qui constituera le point de départ de la politique de sécurité des SI des EPLE, afin d'engager rapidement les opérations liées aux charges revenant aux collectivités instaurées par la loi de 2013.

Patrick BENAZET rappelle quelques éléments de contexte :

- Une coopération forte entre les collectivités et l'académie : les travaux menés depuis plusieurs mois et notamment l'accord-cadre qui a été signé par 5 collectivités sur 6, en sont la preuve.
- Cette démarche s'inscrit dans le cadre d'un contexte juridique que va exposer Thierry LAVIGNE, Directeur des affaires juridiques ;
- L'émergence d'attaques difficiles à appréhender pour les acteurs de la sécurité rend les choses complexes ;
- Le document mis en cible des travaux devra tenir compte du périmètre académique en relation avec le périmètre de la région académique qui est désormais étendu, bien que les 3 académies conservent leur propre existence.

Introduction du séminaire par la RSSI du ministère

Dominique ALGLAVE
RSSI du ministère

Dominique ALGLAVE salut l'ensemble des participants et remercie Patrick BENAZET de l'avoir invité à un événement de cette importance. Le ministère avance avec des premiers de cordée et cette convention constitue une première initiative importante. Le ministère aura l'occasion de demander à Patrick BENAZET de présenter cette démarche au cours des journées thématiques nationales à venir. L'aspect de coconstruction est intéressant, la parole n'est pas préétablie et la manière de la conduire est très importante. On va donc essayer ensemble de trouver le bon tempo et la bonne dose qui va permettre de définir un cadre cohérent qui va nous amener à avoir une meilleure SSI.

Par ailleurs, le contexte très porteur (250 000 machines touchées par la récente cyber attaque avec plus d'une centaine de pays concernés) nous pousse à trouver un cadre qui protège les usagers, les ayants droits et les bénéficiaires de nos SI.

Au sein du ministère, on pratique par dialogue contradictoire notamment dans le domaine de la SSI. Cette méthode permet de mieux définir quelque chose qui n'est pas forcément connu ou de mieux l'appréhender. Tant qu'on reste en contradiction le dialogue est fécond. Au ministère, il y a également une AQSSI (Autorité Qualifiée pour la SSI), chaque entité ayant une AQSSI.

Pour l'ensemble de l'académie, le recteur a désigné une autorité d'homologation qui autorisera ou pas la mise en service d'une portion du SI ou qui demandera à l'autorité d'homologation de délivrer une autorisation temporaire. C'est dans ce cadre-là qu'on ira vers une sécurité accrue pour faire face à des forces de destruction massive (le mot cyber menace est désormais galvaudé). Cette instance nous permettra en outre de dialoguer.

Patrick BENAZET remercice le RSSI du ministère et indique qu'il est tout à fait naturel d'avoir associé le RSSI national pour pouvoir bénéficier de son expérience. Il lui semblait également important que cette approche, jusqu'à présent très technique, soit éclairée par la vision du directeur des affaires juridique.

1. Le cadre réglementaire de la compétence partagée

Thierry LAVIGNE,
Directeur des affaires juridiques

Pendant longtemps les communes ont financé en grande partie la construction des établissements scolaires, l'Etat assurant le fonctionnement. Avec la loi HABY du 11 juillet 1975 qui leur a conféré le statut d'établissements nationaux, l'Etat prend en charge l'ensemble des dépenses de fonctionnement et d'investissement pour faire face à la hausse de la demande de scolarisation sous l'effet conjugué du babyboom et de la prolongation de la scolarité obligatoire jusqu'à 16 ans.

Avec la loi du 22 juillet 1983 portant répartition des compétences entre les communes, les départements, les régions et l'Etat, une nouvelle catégorie d'établissement est créée : l'EPLE.

Avec la loi du 13 août 2004 relative aux libertés locales, de nombreux pouvoirs sont transférés aux collectivités territoriales. Le dispositif s'inspire des lois Jules Ferry sur l'enseignement primaire : à l'Etat, le service d'enseignement proprement dit, aux collectivités territoriales, la construction et le fonctionnement des établissements scolaires auxquels se sont ajoutés au 1er janvier 2005, l'accueil, l'hébergement, la restauration, l'entretien technique et le transfert correspondant des personnels techniques.

Pour le législateur, la formalisation de cette cogestion passe par la mise en place d'une convention bilatérale signée par le chef d'établissement et le président de la Collectivité Territoriale de Rattachement (CTR) qui fixe les modalités de leurs compétences respectives. La convention apparaît ainsi comme un instrument de dialogue direct et privilégié entre les deux partenaires.

Un palier législatif supplémentaire de la cogestion de l'Education est franchi avec la loi de programmation pour la refondation de l'école de la République du 8 juillet 2013.

La loi double la représentation de la CTR dans le conseil d'administration de chaque EPLE.

Si elle le souhaite, la CTR peut être cosignataire du contrat d'objectif conclu entre l'EPLE et le rectorat. Surtout, la loi clarifie sans la modifier, la répartition des compétences entre l'Etat et les CTR en matiére d'équipement informatique.

En application de l'article L.211-8 du code de l'Education, les dépenses de fonctionnement pédagogiques en matiére de ressources numériques incluant les contenus et les services, sont à la charge de l'Etat.

En revanche, en application des articles L.213-2 et L.214-6, il est rappelé que les départements et les régions ont la charge de l'acquisition et de la maintenance des matériels informatiques et des logiciels prévus pour leur mise en service nécessaires à l'enseignement et aux échanges entre les membres de la communauté éducative (équipements actifs réseaux, serveurs de données, terminaux, matériels de sécurité).

Ces dispositions législatives ne nécessitant aucun décret d'application, c'est le mode conventionnel qui demeure l'instrument privilégié de la mise en oeuvre concréte de l'organisation de la maintenance, de l'assistance technique par l'académie et les CTR. La coordination est également essentielle en matiére de sécurité. Les incidents de sécurité sur les systémes d'information sont de nature à altérer et détruire des informations sensibles.

Les enjeux sont majeurs en raison du nombre de personnes concernées : 12 millions d'éléves et d'apprentis, un million de personnels enseignants et administratifs, 65 000 éléves, colléges et lycées.

Si les équipements de sécurité constituent une dépense obligatoire pour les collectivités, la sécurité des systémes d'information (SSI) est placée sous la responsabilité de l'Etat, en vertu de son pouvoir de police qu'il ne peut pas déléguer.

IL existe ainsi une chaîne fonctionnelle de sécurité qui va du niveau ministériel jusqu'à l'EPLE dirigé par un chef d'établissement, représentant de l'Etat dans son établissement et responsable des biens et des personnes, qui peut prendre des mesures conservatoires d'accés à l'établissement, des mesures de prévention y compris dans le domaine de la sécurité informatique.

Cette chaine de sécurité repose sur un haut fonctionnaire de défense et de sécurité, assisté d'un fonctionnaire de sécurité des systémes d'information, en lien avec la DNE, qui est relayée au niveau académique, par une Autorité Qualifiée pour la SSI, le recteur.

L'expertise repose, au niveau académique, sur un RSSI, qui a été nommé et mandaté par le recteur, pour mettre en place toute la politique de référentiels réglementaires et légaux suivante :

- La politique de SSI de l'Etat (PSSIE) fait l'objet de la circulaire qui fixe un ensemble de régles de protection applicatives aux SSI de l'Etat. Le 17 juillet 2014, la PSSIE s'applique à tous les SI de l'Etat, aux établissements publics sous tutelle ministérielle et aux services déconcentrés. Elle concerne l'ensemble des personnes qui interviennent dans les SI de l'Etat ou encore des tiers qui interviennent pour le compte de l'Etat. Les destinataires sont les DSI en particulier et toutes les personnes chargées de l'exploitation des SI.
- La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux traitements de données automatisés ou non, à caractére personnel, contenues ou appelées à figurer dans des fichiers.
- Le référentiel général de sécurité est prévu par l'article 9 de l'ordonnance du 8 décembre 2005 et son décret d'application du 2 février 2010 fixe les régles auxquelles les systèmes d'information mis en place par les autorités administratives (administrations de l'Etat, collectivités territoriales) doivent se conformer pour assurer la sécurité des informations échangées, leur confidentialité et leur intégrité.

Au niveau académique, l'élaboration et l'organisation du SI doivent être réalisées en cohérence avec les exigences de sécurité décrites dans les dispositifs législative et réglementaire qui viennent d'être évoqués.

Il appartient ainsi à l'autorité académique qui dispose d'un référentiel académique des exigences de sécurité applicable dans les établissements scolaires de s'assurer de la conformité des dispositifs de sécurité mis en place par les collectivités de rattachement.

A beaucoup d'égards, tout est à faire en matiére d'apprentissage et de culture de la sécurité des SI. C'est donc une extrême vigilance de tous les instants en la matiére qui doit guider l'action de l'Etat et des collectivités à travers un dialogue permanent formalisé sur un mode conventionnel.

Patrick BENAZET remercie Thierry LAVIGNE pour ce cadrage juridique et ces deux phrases de conclusion, la parole est donnée à la salle.

Yves NIVELLE, Conseil départemental de la Gironde, remercie pour ce rappel juridique et cette lecture de l'histoire qui a conduit au partage des compétences ETAT/CT. Sa question porte plutôt sur le référentiel des exigences concernant notamment page 5 - le paragraphe 4 relatif aux ENT, idem pour la partie «logicielle». Il souhaiterait avoir l'avis du directeur des affaires juridique car il s'étonne de cette conclusion compte tenu des travaux menés en co-construction avec d'autres partenaires, la caisse des dépôts notamment.

Thierry LAVIGNE réitère que les charges relatives aux ENT relèvent de la compétences des collectivités.

David BELBES, Conseil département du Lot-et-Garonne, partage les interrogations d'Yves NIVELLE. Autant il n'y a pas de doute possible sur les matériels et les infrastructures, autant la partie concernant les ENT et les logiciels n'est pas explicite. Il a d'ailleurs été question que les ENT continueraient à être portés par l'Etat partout où les collectivités ne s'engageraient pas.

Patrick BENAZET indique que la DAJ du ministère a été saisie à deux reprises sur cette question. Deux notions se font front dans l'arsenal juridique dont on dispose. La collectivité a la charge, sous-entendu financière, ce qui ne signifie pas qu'elle a la compétence au sens juridique. Dans les articles 19, 21 et 23 de la loi de 2003 qui font état de la charge qui revient à la collectivité et à l'Etat, on se rend bien compte qu'on est sur une compétence partagée.

C'est pour cela que concernant l'ENT LéA proposé par la région, des conventions ont été mises en place entre la Région, l'académie et l'EPLE et que ces différents partenaires participent aux comités d'exploitation. Actuellement l'ENT pour les collèges est ARGOS. Il est proposé par l'académie ce qui est une originalité par rapport au droit. Cependant se mêlent des compétences à la fois de sécurité, technique, etc. Des travaux ont été lancés il y a un peu plus de 6 mois avec les collectivité ayant choisi l'ENT des écoles ALIENOR pour assurer un continuum entre le primaire et le collège (cycle 3), travaux poursuivis désormais avec l'ensemble des collectivités départementales.

La réponse est sans ambiguïté : répartition de la charge à préciser dans les conventions mais les collectivités n'avancent pas toutes à la même cadence, elles n'ont pas toutes les mêmes moyens. L'essentiel étant que la mise à disposition des ENT soit réalisée dans les meilleures conditions sur l'ensemble du territoire, démarche que l'Etat ne peut mener seul.

La délivrance de services pédagogiques, si elle incombe à l'Etat, doit se faire au travers d'un service qui s'appuie sur un systéme d'authentification et de fédération d'identité, domaine à la charge de l'ensemble des acteurs. Par ailleurs, l'accord-cadre signé porte, au plan académique, sur une phase transitoire qui a été fixée à 3 ans.

Thierry LAVIGNE confirme que les ENT font partie des outillages informatiques au même titre que d'autres équipements à la charge des CTR.

Patrick BENAZET rappelle que la définition de l'ENT est posée dans le cadre du SDET.

Jean-Louis BRUNEL fait part des difficultés rencontrées par le responsable du département «systéme et réseau» d'Aix-Marseille à travailler avec les collectivités du fait des questionnements liés aux textes réglementaires. Il invite les participants à consulter réguliérement le site legifrance.gouv.fr sur lequel les textes sont consultables dans leurs différentes versions.

Si la loi a évolué il ne nous appartient pas de discuter des textes, mais nous devons les rappeler. C'est faire preuve d'intelligence collective que de mettre en place ces textes en tenant compte des difficultés du terrain.

Dominique ALGLAVE cite, à titre d'exemple, la mise en place du GAR (Gestionnaire d'Accés aux Ressources). Il faudra bien homologuer la totalité du service rendu pour déployer ce service numérique éducatif pour tous.

Patrick BENAZET considère que cette nouvelle brique de la PSSI académique qu'est le référentiel des exigences de sécurité s'est construite un peu à marche forcée, devant la volonté de certaines collectivités d'aller jusqu'à la maîtrise du SI de l'EPLE.

Certaines collectivités ont décidé de faire des POC (Proof of Concept) pour orienter leurs choix en matiére d'architectures matérielles.

A l'issue de la phase transitoire fixée par l'accord-cadre, il est prévu que les collectivités assurent totalement leurs responsabilités au sens de la loi. Une premiére approche aurait été de donner des consignes techniques de techniciens à techniciens mais cela aurait été la meilleure façon de ne pas parvenir à un cadre stratégique formalisé. Il est apparu nécessaire de marquer un temps de pause pour proposer un espace de coconstruction qui intégre ce rôle régalien en prenant en compte ce qui est transférable et ce qui reste du rôle de l'Etat dans son rôle de police.

Il s'agit du référentiel des exigences de sécurité qui a été élaboré et qui fera l'objet d'une mise à jour au moins une fois par an.

2. Le référentiel académique des exigences de sécurité pour les EPLE

Lionel LOPEZ,
RSSI Adjoint

Dans ce référentiel on trouve l'ensemble des textes en vigueur ainsi que des recommandations, l'objectif étant d'être exhaustif pour prendre en compte tous les besoins des collectivités et de l'Etat de façon détaillée et de mettre en place les règles de sécurité dans les EPLE. On s'efforce de les faire respecter mais parfois il y a quelques entorses. Il se veut également évolutif et pourra être modifié si de nouvelles technologiques ou de nouvelles règles apparaissent.

Enfin il est contraignant, certaines régles étant non négociables car relèvent de l'autorité du recteur.

Les différentes exigences techniques ont été regroupées par chapitre en fonction des besoins et des acteurs concernés (cf diaporama). Un focus sur les réseaux wifi a été fait car il ne doivent en aucun cas être installés sur le réseau administratif, or c'est l'élément le plus difficile à maîtriser. Seul le plan d'adressage est imposé, celui de Racine, qui est défini au niveau national et qui doit être respecté pour garantir la continuité de service.

Dans les EPLE, 98 % des usagers sont des mineurs. Il est donc trés important de filtrer les accés à des sites illicites. Un deuxième focus concerne la journalisation du trafic, il est important de tracer tout ce qui se passe sur le réseau pour que l'AQSSI puisse y avoir accés en cas de réquisition judiciaire.

Ce référentiel décrit les exigences mais n'impose pas les solutions techniques.

Il rappelle les bonnes pratiques. C'est un outil qui va permettre de garantir le même niveau de sécurité dans tous les EPLE de l'académie sur la base d'informations identiques.

Concernant sa mise en place :

- Avant la loi de 2013 : l'académie s'occupait de toutes ces régles ;
- Durant la phase transitoire : les collectivités commencent à prendre la main dans le cadre de la continuité de service ;
- A l'issue de la phase transitoire : les collectivités les mettent en oeuvre, le recteur, AQSSI, doit pouvoir accéder à toutes les traces sans devoir passer par des tiers.

Patrick BENAZET insiste sur le devoir de fixer le même niveau de sécurité pour tous les élèves scolarisés dans le système éducatif. Ce point est très important pour l'exercice du contrôle dans un contexte de partage de la responsabilité.

A partir du moment où une collectivité a pris le contrôle dans le cadre d'une procédure d'homologation, il est indispensable que l'outillage retenu soit très clairement annoncé et accessible par l'autorité académique. On peut faire une analogie avec les autoroutes : l'Etat concède leur construction à un prestataire puis envoie la gendarmerie contrôler leur bonne utilisation.

Jean-Louis BRUNEL souhaite ajouter une précision concernant la problématique des logs car le pôle est souvent sollicité par l'autorité judiciaire pour communiquer des logs, qui sont parfois opérés par des prestataires extérieurs. S'il y a un problème dans une école, l'autorité judiciaire interroge le recteur qui doit les communiquer rapidement car nul ne peut faire obstacle à la justice. Cela pose deux questions : Comment enregistrons-nous les logs ? Comment les traitons-nous ? L'article 31.1 du CPCE (Code des Postes et Communications électroniques) impose au F.A.I. de fournir les logs.

Sommes-nous F.A.I. vis-à-vis de nos utilisateurs ? Le fait est que l'autorité judiciaire se base sur cet article pour nous demander les logs. L'Etat s'est donc mis dans cette position pour pouvoir répondre. D'après le règlement européen sur la protection des données, le législateur désigne aujourd'hui une coresponsabilité.

Franck PUIROUX, CD de la Gironde, pose une question qui peut paraître un peu polémique. Le terme employé auparavant était « recommandations », désormais on parle d' « exigences », comme si l'Etat semblait ne pas avoir de pouvoir vis-à-vis des EPLE.

Patrick BENAZET confirme que l'Etat a toujours eu des exigences en matière de sécurité, sauf qu'une sorte de délégation était établie entre les services rectoraux et les EPLE. Ces exigences sont héritées d'un schéma directeur appelé S2I2E, qui commence à être un peu vieux. Ce qui a changé, c'est que ces exigences sont transférées vers les collectivités et que le rôle régalien de l'Etat doit être porté à la connaissance de celles-ci.

Florence ALMONACID, CD des Pyrénées-Atlantiques, demande si les EPLE sont informés de ces différentes conventions et référentiels qui lient le rectorat aux collectivités.

Patrick BENAZET la remercie de cette remarque fort judicieuse, il a obtenu récemment l'accord du recteur pour organiser un séminaire sur la sécurité à destination des chefs d'établissement.

Lorsqu'il s'est agi de publier l'accord-cadre il a été d'abord question d'une médiatisation mais le recteur a pensé qu'il fallait attendre la signature des conventions bilatérales pour le faire. Bien sûr il va falloir communiquer pour que le chef établissement n'apprenne pas par la bande qu'il existe des textes qui s'appliquent dans son établissement et qu'il a un rôle en tant que personne juridiquement responsable. Il a besoin de savoir qui fait quoi et à qui on s'adresse. C'est pour cela qu'on a évoqué un dispositif d'assistance mutualisé avec un guichet unique. Par ailleurs, la mise en place d'un dispositif d'assistance mutualisé avec Limoges et Poitiers est en cours, qui concernera, dans un premier temps, les lycées de la région académique Nouvelle-Aquitaine.

Alexandre SEUNES, CD de la Dordogne, souhaite illustrer la très grande méconnaissance des EPLE. Ce matin un gestionnaire a appelé pour savoir si ce que SCOL-TELESERVICES disait était vrai sur l'obligation de mettre un mot de passe pour accéder à internet depuis un poste du CDI.

Cet exemple démontre la nécessité d'une cohésion entre collectivités et Etat. L'objectif est d'assurer la sécurité. Ce travail de coconstruction est donc nécessaire. Son département essaie de voir comment il va s'organiser sachant que les charges ont été transmises sans attribution de moyens, et qu'il y a beaucoup à faire. L'important est de bien s'entendre sur le discours à tenir vis-à-vis des établissements.

Patrick BENAZET acquiesce : il faut s'entendre sur le discours et le prononcer d'une seule voix. C'est pourquoi il invitera les collectivités à coconstruire le contenu du séminaire à destination des chefs d'établissement.

Thierry LAVIGNE souligne qu'il peut y avoir des impacts devant le juge. Tous les acteurs doivent donc être parfaitement informés.

Patrick BENAZET indique que la chaine des acteurs est importante à prendre en considération, il faut avoir une idée de ce qui est en place pour pouvoir nous projeter vers ce qui le sera à l'avenir.

3. Les chaînes d'alerte et opérationnelle

Laure COULON,
RSSI Adjointe

La chaine d'alerte fonctionne particulièrement bien au ministère de l'Education nationale et doit être confortée.
La responsabilité des parties, suite à la loi de 2013, est reprécisée de façon synthétisée dans un schéma présenté aux participants.

Concernant la responsabilité des acteurs : une partie est opérationnelle depuis plusieurs années, il s'agit de celle concernant le recteur en qualité d'AQSSI. Ce qui est visé ici, c'est notamment le lien avec le correspondant sécurité des collectivités. Ses coordonnées doivent être connues par l'autorité académique, il rend compte à sa collectivité mais aussi à l'autorité académique. Inversement le responsable sécurité de l'Etat peut être amené à rendre compte à la collectivité si l'incident touche son périmètre.
Rappel concernant la chaine d'alerte : en cas d'incident le RSSI de l'académie doit être informé et c'est lui qui est chargé d'escalader aux niveaux supérieurs.

Patrick BENAZET concède que ce document est loin d'être parfait, notamment sur la terminologie employée.

Domique ALGLAVE souhaite apporter un petit éclairage sur rôle de l'AQSSI. Comme les mots le disent bien AQSSI c'est une autorité qui autorise ou qui n'autorise pas. Les responsables sont amenés à répondre, après avoir collecté les informations sur les éléments. Nous avons tous la même autorité. Nous rendons une réponse que nous construisons ensemble.

Vu la voilure que nous avons, nos chaines d'alerte sont très performantes. Cette performance est éprouvée avec l'arrivée des services numériques car les alertes de sécurité se multiplient et notre périmètre s'élargit à de nouveaux cas. 15 ou 20 événements dans une académie peuvent passer inaperçus mais au niveau national ces évènements sont généralisés et si les informations remontent au cabinet du ministre c'est parce qu'au niveau local quelqu'un n'a pas pris la mesure de l'évènement.

Dominique ALGLAVE constate qu'il est de plus en plus judicieux de positionner le RSSI au sein d'une DSI. Toutes les nominations actuelles vont dans ce sens. Dans notre ministère, c'est efficace. Il pense que vu les temps vers lesquels nous allons, il est très important de disposer de ressources opérationnelles.

Jean-Louis BRUNEL rappelle que, dans ce domaine, ce que nous visons c'est l'efficacité de notre action. Il évoque l'article 86 de l'instruction générale interministérielle 1300 qui définit les fonctions de l'autorité qualifié SSI, à savoir mettre en œuvre la PSSI, veiller et faire contrôler les règles, nommer et mandater l'autorité d'homologation, nommer un RSSI. En dernier ressort c'est l'AQSSI qui a la responsabilité du traitement des données dans l'académie. La responsabilité du recteur est donc énorme et, à ce titre, il a des exigences de la part de ses services techniques.

Franck PUIROUX, Conseil départemental de la Gironde, indique qu'il y a un certain nombre de bornes wifi dans les collèges de la Gironde. Comment le recteur fait-il pour qu'elles disparaissent ?

Patrick BENAZET indique que le rectorat dispose d'un système automatique d'alerte car il n'a pas forcément l'information de la part du chef d'établissement. Cette semaine une réquisition est arrivée suite à un accès via une borne wifi. Le chef d'établissement n'était peut-être pas informé. Des choses se passent actuellement parce que des acteurs de terrain agissent selon une préoccupation ou un bon vouloir mais pas dans un cadre formel connu.

Cela pose la question de la verticalité des acteurs. Il faut parvenir à une unité de commandement qui s'inscrive dans les prérogations des collectivités tout en veillant à la bonne résolution des problémes.

Patrick BENAZET a proposé au recteur il y a 15 jours la mise en place d'un COS (Centre Opérationnel de Sécurité), il faut qu'il soit connu par les collectivités, qu'il soit légitimé et qu'il ait la garantie d'avoir leurs retours d'information. On reçoit environ 25 alertes « borne wifi » par jour mais aujourd'hui cela ne fait pas sens car la chaine d'alerte n'est pas informée et il n'y a donc pas d'action efficace.

On est sur un mode militaire, face à une attaque. Il faut fabriquer une unité de sécurité à l'intérieur de laquelle on va retrouver tous les acteurs opérationnels.

Comment mettre le dispositif sous contrôle d'une instance unique, qui peut être pilotée par un organe multicéphale, qui fasse que quand un ordre arrive, il soit perçu comme non discutable d'où qu'il provienne.

Cette instance est à créer en collaboration, tout est ouvert, toutes les idées sont les bienvenues. Cela peut faire l'objet d'un groupe de réflexion via un espace collaboratif.

Dominique ALGLAVE rappelle que lorsqu'on a connaissance, par exemple, du fait qu'un « cryptolocker » est en train de s'introduire dans nos serveurs, la chaine d'alerte doit demander une posture, le responsable de celle-ci n'ayant pas l'autorité pour décider de débrancher les dits-serveurs. Par contre l'AQSSI a cette autorité mais il n'a pas la compétence technique donc il écoutera son RSSI pour prendre sa décision. Son acte de responsabilité consiste à nommer un RSSI. De même, le HFDS a décidé de nommer des autorités d'homologation, mais ensuite les actes techniques reviennent aux RSSI. Ce que Patrick BENAZET propose de mettre en place est essentiel pour faire ce qu'on a à faire mais aussi pour pouvoir en répondre.

4. La procédure d'homologation

Jean-Louis BRUNEL,
Chef du pôle national de compétence SSI

La question qui s'est posée est comment cadrer les choses au niveau académique en matiére d'homologation comme cela a été fait pour le référentiel des exigences de sécurité.

Le document proposé dans le dossier distribué aux participants (Référentiel d'homologation de l'académie de Bordeaux) ne fait pas l'objet d'une diffusion restreinte mais il s'agit d'une version V1.

Le recteur a nommé un RSSI académique le 1er mai 2015, Patrick BENAZET puis 2 adjoints, Laure COULON et Lionel LOPEZ. Il a également nommé une autorité d'homologation il y a environ 18 mois : Patrick BENAZET.

Le fait d'avoir réparti les autorités d'homologation au niveau central par grandes directions du ministère nous amènera peut être à revoir ce dispositif.

Aujourd'hui l'autorité d'homologation va autoriser ou pas, mais sous quelle forme ?

Une erreur s'est glissée sur la diapo 22 : il s'agit d'arriver à une attestation d'homologation et non à un certificat. Les parties prenantes sont les suivantes : chefs d'établissement, sous-traitants et collectivités. Les personnes qualifiées sont les experts des domaines métier, technique et organisationnel. La commission rassemble l'ensemble des acteurs.

C'est une première opération de portée académique, qui ne s'inscrit pas dans un cadre de référence national.

L'équipe RSSI a néanmoins pris soin d'appuyer ses travaux sur le pôle de compétence d'Aix-Marseille et j'ai naturellement participé à la rédaction du document.

Cela va impacter directement les collectivités dans le champ des composants en partant du choix jusqu'à la mise en œuvre, tout en restant dans des choses réalisables.

Jean-Louis BRUNEL souhaite qu'on se mette d'accord sur les termes.

Qu'est-ce qu'une attestation d'homologation ? C'est une entité qui atteste auprès de ses utilisateurs que les risques qui pèsent sur eux et sur les informations qu'ils manipulent sont connus et maîtrisés.

Pour qu'ils soient connus, il faut qu'ils aient été identifiés (impact métier, impact d'une fuite de données, atteinte à l'intégrité d'une donnée, etc..) puis il faut les apprécier. Apprécier la probabilité de menace et de risque constitue l'étude de risque.

Par rapport à ces risques-là on définit des objectifs de sécurité :

- l'éviter,
- le transférer,
- l'accepter,
- le réduire (mesures technique et organisationnelle pour le ramener à un risque résiduel acceptable).

Auditer les mesures mises en place consiste à en vérifier l' « auditabilité » et l'efficience (robustesse).

Une attestation formelle permettra d'indiquer que le processus a été mis en place.

Un certificat est attaché à un produit. Il vérifie que ce produit répond à des exigences techniques.

L'homologation est avant tout attachée à l'utilisateur, elle lui garantit qu'il peut utiliser le produit en toute sécurité.

Jean-Louis BRUNEL cite l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ainsi que le décret pris en application et notamment les articles 9 (RGS), 10 (certificat électronique) et 12 (produits et services de sécurité). Enfin il évoque la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Tout ce qui fait l'objet d'une utilisation de données à caractère personnel (DCP) doit faire l'objet d'une homologation, notamment pour les télé-services.

Le réglement européen nous demandera en plus de faire l'étude d'impact. L'ANSSI nous dit qu'il faut tous les homologuer, ce qui représente 3 000 ou 4 000 homologations dans l'Education nationale, homologations qui ne seront pas terminées en 2018.
Les questions qui se posent sont :

- comment se met-on en ordre de marche ?
- quelle stratégie d'homologation met-on en œuvre ?
- comment nous-allons assurer ces procédures d'homologation ?

Le risque est d'être trainé devant les tribunaux par les usagers si nos télé-services ne sont pas homologués. Un SI ne se réduit pas à sa composante informationnelle, mais aussi à ses composantes humaine et technique. Question à se poser : est-ce un simple composant technique qu'on introduit dans l'infrastructure ou est-ce un composant SI ? S'il y a introduction d'un composant : il faut faire une demande d'avis, s'il y a introduction d'un SI, il faut demander une homologation.
On peut adapter les études de risque en fonction du SI à homologuer, par exemple en fonction du nombre de personnes ou de données déclarées sensibles par la CNIL.

L' objectif est que les membres permanents et les membres « partie prenante » invités constituent la commission d'homologation. L'ANSSI fait partie des membres invités de droit.
Concernant les décisions possibles, elles peuvent être les suivantes :

- Refus : on ne doit jamais arriver à ce cas ;
- Attestation provisoire d'exploitation car on est bloqué par des exigences opérationnelles : on se le dit et on se donne un délai pour corriger les risques ;
- Attestation définitive valable 3 à 5 ans au maximum.

Dominique AGLAVE doit quitter la réunion pour rentrer à Paris. Il remercie tous les participants du travail commencé qui devrait apporter des aspects fructueux pour le ministère.

Patrick BENAZET estime important qu'on ait un canal d'échanges qui fasse, qu'à un moment donné, on puisse se dire que c'est bon pour les 2 parties.

Actuellement les commissions d'homologation homologuent uniquement des SI de l'Education nationale. Par ailleurs, la demande d'avis correspond à une procédure hyper simplifiée.

Il est possible que ce référentiel fasse l'objet d'un pointage dans les conventions bilatérales. Il s'agit d'un document totalement amendable, qui constitue un cadre de référence.

Il fait part d'une difficulté avec la Région, liée à la nécessité de travailler de concert, le recteur de région académique étant délégué de la zone sud-ouest.
Il faut arriver à produire un cadre de sécurisation pour les responsables que nous sommes.
Parmi les acteurs de la chaine de responsabilité il y a bien évidemment les ADSI pour lesquels il est indispensable de fixer le cadre de travail. On a préparé la charte de l'administrateur systèmes et réseaux qui sera soumise au prochain Comité Technique Académique. Suite à quoi on réunira les acteurs concernés pour leur expliquer leurs droits et leurs devoirs.
Patrick BENAZET propose aux collectivités de travailler sur ce référentiel que l'on l'incorpore ou pas aux conventions.

A la question de savoir pourquoi l'homologation ne serait pas désormais du ressort des collectivités, Jean-Louis BRUNEL apporte l'élément de réponse suivant : le risque vise essentiellement les usagers des EPLE qui dépendent plus grandement de l'Education nationale de par leur mission pédagogique
On est néanmoins dans un domaine partagé. Si la collectivité veut aller au-delà de la demande d'avis, elle pourra le faire dans un cadre sécurisé.
Concernant le problème des bornes wifi, il faut essayer de ne pas être confronté à ces situations, de les anticiper pour ne pas devoir prendre de décisions coercitives.
L'objectif est d'avoir un cadre qu'on commence à s'appliquer à soi-même.

La parole est donnée à la salle.

Alexandre SEUNES : quand on regarde le fonctionnement des établissements, on est très loin de la réalité.
Si on s'entend sur une cible, cela ne peut se faire que via une collaboration forte au travers d'ateliers, y compris sur des questions techniques. Une difficulté repose sur le périmètre qui augmente très rapidement dans les établissements. Comment assure-t-on la sécurité et la modernisation ?

Patrick BENAZET adhère au fait qu'il faille se rapprocher des usages. Notre ministère s'est doté d'un organe, les DAN, qui n'existe dans aucune entreprise. L'enjeu est très fort, mais leur rôle en la matière reste assez faible. Il repose sur une mission de conseil. Il faut voir les choses sous un aspect qui n'est plus techniciste. Les enjeux de la SSI passent par l'acculturation. C'est pourquoi un plan de communication a été mis en place à la DSI qui se veut de porter de l'information jusqu'au fin fond de la ruralité.

La pédagogie repose sur un principe difficile à cerner pour un RSSI : celui de la liberté. Les enseignants doivent pouvoir faire un cours dans un cadre bien connu, il y a donc des enjeux de moyens.

Il est difficile de les freiner s'ils veulent organiser une séance pédagogique avec des outils numériques qui sortent du champ d'un schéma dont ils n'ont aucune connaissance. Les usages nous précéderont toujours.

Patrick BENAZET est preneur si les collectivités territoriales ont des remontées d'information des EPLE.
Il souhaiterait entendre la Région s'exprimer.

Thierry-Paul COTON, RSSI du Conseil régional, indique prendre l'information communiquée ce jour. Il informe que la région dispose d'un processus d'homologation et s'interroge sur le processus à utiliser pour homologuer l'ENT LéA ?

Patrick BENAZET estime que nous nous inscrivons dans un groupement de confiance. Ainsi, dès lors qu'un composant est ajouté par une des parties, il doit être homologué par cette partie.
LéA doit donc l'être par la Région et le Président de la Région devrait en supporter les conséquences si cela n'était pas fait. Se pose la question d'un système dont on ne sait pas qu'il n'est pas homologué.

Patrick BENAZET clôt la séance à 17 h 25, en précisant que les échanges peuvent se poursuivre par mail. Il informera notamment les collectivités de l'évolution du projet de COS inter-académique. Concernant la question d'un réseau RSSI, l'idée est soumise. Il est prêt à s'investir personnellement dans la réflexion de la structuration d'un éventuel club RSSI.

Il réaffirme le plaisir qui a été le sien et celui de l'équipe SSI académique d'échanger sur cette thématique avec les collectivités, remercie les participants pour avoir fait le déplacement et rappelle que la prochaine étape concerne la finalisation des conventions bilatérales et la mise en œuvre de la PSSI opérationnelle. Concernant l'éventualité d'un commandement unique, il rappelle que cela ne signifie pas que l'académie va prendre la main mais que lorsqu'un ordre sera passé il le sera dans le cadre d'un canal officiel unifié.

Les perspectives

En prolongement de ce séminaire, les participants ont acté la volonté d'engager la formalisation d'une chaine opérationnelle qui intégrera l'Etat, les CT et les EPLE. Cette chaine bénéficiera des effets du Centre Opérationnel de Sécurité (COS) que l'académie envisage de mettre en place.

RÉGION ACADÉMIQUE
NOUVELLE-AQUITAINE

MINISTÈRE
DE L'ÉDUCATION NATIONALE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION