TECHNICIEN TERRITORIAL PRINCIPAL DE 2ème CLASSE

CONCOURS EXTERNE

SESSION 2014

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.

- Aucune référence (nom de collectivité, nom de personne, …) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.

- Seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou pour souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.

- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 29 pages

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué

Vous êtes technicien territorial principal de 2 ème classe à la direction des systèmes d'information de la commune de Techniville qui compte 50 000 habitants.

Cette direction, qui vient d'achever son premier Schéma Directeur Informatique (Modernisation de ses équipements, apport de la mobilité pour les monades, nouvelles applications métier, e-services pour les administrés, dématérialisation de certains flux avec d'autres établissements publics…), souhaite maintenant mettre en œuvre un projet pluriannuel en matière de sécurité.

Dans cet objectif, le Directeur des Systèmes d'Information vous demande dans un premier temps de rédiger à son attention, exclusivement à l'aide des documents ci-joints, un rapport technique présentant un état des lieux en matière de sécurité informatique dans les collectivités territoriales.

08 points

Dans un second temps, vous lui proposerez un plan d'action en vue d'assurer la sécurité informatique à l'échelle de Techniville, en tenant compte des enjeux et des contraintes (techniques, juridiques, humaines et financières).

12 points

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

Liste des documents joints :

Document 1 : « Le niveau de sécurité informatique des collectivités s'améliore mais reste perfectible » - *Site www.blog.grandesvilles.org* – juillet 2012 – 1 page

Document 2 : « Encore des efforts à faire pour la sécurité informatique des collectivités locales ? » *Site www.technicites.fr* – juillet 2012 – 1 page

Document 3 : « Les données informatique des collectivités locales ne sont pas assez protégées » - *La Gazette des Communes* – janvier 2013 – 2 pages

Document 4 : « Les collectivités ont des pratiques inégales en sécurité informatique » - *Rubrique Collectivités Territoriales du site www.weka.fr* – mars 2013 – 1 page

Document 5 : « La prévention des risques informatiques » - *Le guide Info Maires* – septembre 2012 – 2 pages

Document 6 : « Archivage électronique sécurisé » - *Site de l'ANSSI* – 2012 – 5 pages

Document 7 : « 10 conseils pour la sécurité de votre système d'information » - *CNIL* – 2 pages – 12 octobre 2009

Document 8 : « Le Référentiel Général de Sécurité » - *Portail de la Modernisation de l'Etat* – 2 pages – mars 2010

Document 9 : « Le Référentiel Général de Sécurité et les certificats de signature électronique » - *Site www.economie.gouv.fr* – mai 2013 – 4 pages

Document 10 : « La sécurité informatique trop souvent l'affaire de la seule DSI ? » - *Rapport du CLUSIF* – février 2013 – 3 pages

Document 11 : « Politique de sécurité des systèmes d'information » - *Site de l'ANSSI* - Octobre 2011 - 3 pages

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

Le niveau de sécurité informatique des collectivités s'améliore mais reste perfectible

18 juillet 2012

Le Clusif a mené une enquête auprès de 205 collectivités (dont 34 agglos) sur leur politique en matière de sécurité informatique. Le premier constat de cette enquête est une baisse de la sinistralité, reflet des efforts faits par les collectivités pour sécuriser leur système d'information. Ainsi les pertes de services essentiels sont passées de 44 % en 2008 à 27 % en 2012 avec des chiffres identiques en matière d'infections virales.

Des efforts restent cependant à faire car plus d'une collectivité sur deux (54 %) ne dispose d'aucun processus de gestion de la continuité d'activité et à peine 40% d'entre elles pratiquent une fois par an un audit de sécurité. Seule une collectivité sur 10 a un tableau de bord de suivi de la sécurité informatique. Par ailleurs, si la sécurité des postes et réseaux fixes est globalement bien appréhendée (anti-virus, firewall, détection des intrusions…) de gros efforts restent à faire sur la mobilité (smartphone, accès distant au SI).

Selon le rapport, le principal moteur de la mise en place d'une politique en matière de SSI reste l'existence d'obligations réglementaires avec en particulier l'application du référentiel de sécurité (RGS, obligatoire à partir de mai 2013) et la protection des données personnelles. A cet égard on notera que 39% des collectivités ont désormais un correspondant informatique et liberté (CIL). La dématérialisation des procédures – marchés publics, ACTES, HELIOS… - a par ailleurs eu un fort impact dans l'utilisation de systèmes de contrôle d'accès et de certificats pour sécuriser les échanges de données, désormais utilisés dans 60% des collectivités interrogées.

Malgré ces efforts, le chemin reste encore long, notamment pour les petites collectivités qui ne disposent pas de compétences en matière de SSI. Ainsi, en matière de conformité au RGS, seulement 37% affirment avoir un SI conforme ou partiellement conforme, un tiers ne l'étant pas et un autre tiers…l'ignorant.

Encore des efforts à faire pour la sécurité informatique des collectivités locales ?

Date de mise en ligne : 25/07/2012.

La sécurité informatique des collectivités locales reste encore à améliorer : telles sont les conclusions de l'enquête 2012 du C.L.U.S.I.F (Club de la Sécurité l'Information Français) ; ce club est une association à but non lucratif (créée en 1985) d'entreprises et de collectivités réunies en groupes de réflexion et d'échanges autour de différents domaines de la sécurité de l'information : gestion des risques, politiques de sécurité, cybercriminalité, intelligence économique, etc.

Tous les deux ans, le CLUSIF mène une enquête sur la sécurité informatique des différents types d'organisations ; celle de 2012 a été menée de début janvier à mi-mars de la même année auprès de trois cibles :
- Les entreprises de plus de 200 salariés : 351 y ont répondu
- Les collectivités territoriales : 205 y ont participé
- Des particuliers internautes : 1000 y ont répondu issus du panel d'internautes de l'Institut spécialisé Harris Interactive.

Globalement, l'enquête montre une baisse de la sinistralité mais des pratiques encore à améliorer spécialement dans les administrations territoriales ; « ainsi, dans les collectivités sondées, les pertes de services essentiels sont passées de 44 % en 2008 à 27 % en 2012. Ces statistiques sont identiques en matière d'infections virales, sachant que les pannes internes y sont toujours la principale cause de sinistralité... ; par contre, plus d'une collectivité sur deux (54 %) ne dispose d'aucun processus de gestion de la continuité d'activité et 56 % ne mènent aucun audit (même si 40 % mènent un audit au moins une fois par an). De même, l'utilisation du tableau de bord a stagné depuis la dernière enquête : seule une collectivité sur dix déclare avoir mis en en place des outils de ce type »

Bien entendu, ce sont les collectivités de grande taille qui, dotés de moyens humains et financiers plus conséquents, sont les plus performantes ; a contrario, les collectivités de taille moyenne arguent du fait qu'elles ne disposent pas de moyens suffisants (n.b : 39% des collectivités interrogées ne disposent pas de correspondant Informatique et Libertés).

Il est bon de noter, sans toutefois tomber dans un mauvais esprit, qu'un grand nombre de cabinets d'audit informatique sont membre du CLUSIF et que l'échelle de rémunérations des informaticiens territoriaux doit être d'une autre valeur que celle des informaticiens des entreprises.

la gazette.fr

CYBERSÉCURITÉ

« Les données informatiques des collectivités locales ne sont pas assez protégées »

E. Lesquel | France | Publié le 28/01/2013

Dans un entretien accordé à La Gazette lundi 28 janvier 2013, lors du 5e forum international de la cybersécurité, le commandant Rémy Février, chargé de mission intelligence économique à l'état-major de la région de gendarmerie Nord-Pas de Calais pointe du doigt la vulnérabilité des systèmes d'information des collectivités.

Rémy Février est ancien cadre du secteur privé et un ancien dirigeant d'un cabinet de consulting en stratégie. Il est désormais officier professeur sous contrat à la gendarmerie nationale.
Il enseigne l'intelligence économique et territoriale en masters spécialisés à l'école nationale d'administration, en écoles supérieures de commerce et à l'université. Il est également un ancien élu d'une ville de plus de 100 000 habitants.

En matière de cybersécurité, les collectivités sont-elles assez protégées ?

Non, mais il existe très peu de données concrètes et aucune étude au niveau national. De plus, les collectivités sont réticentes à parler des problèmes rencontrés. Cependant, à la vue de mon expérience de terrain et du sondage que j'ai pu réaliser auprès d'une soixantaine de collectivités du Nord-Pas de Calais dans le cadre de ma thèse, les lacunes des collectivités et en particulier des communes dans ce domaine sont énormes. Ces résultats sont transposables à l'ensemble du territoire.

Pourquoi les communes sont-elles les plus vulnérables ?

C'est l'échelon territorial qui détient le plus de données sensibles et c'est aussi souvent là que les moyens pour se protéger sont les plus faibles. Pourtant, que ce soit la prise de contrôle à distance d'un poste de travail, la modification de documents sensibles, l'usurpation d'identité, ou tout simplement la perte de données, la menace est réelle. En cas de problèmes, la responsabilité des élus est clairement engagée.

Un élu peut se retrouver mis en examen pour avoir insuffisamment protégé ses systèmes d'informations ?

Tout à fait. Même si la réglementation dans ce domaine est jurisprudentielle, il ressort clairement qu'un élu, au même titre qu'un chef d'entreprise, peut être mis en examen pour ne pas avoir pris les mesures nécessaires pour se protéger. Or, 70 % des collectivités interrogées ne connaissent pas les responsabilités qui leur incombent !

Les collectivités sont-elles vraiment menacées ?

Avec le développement de l'e-democratie, de l'e-administration, ou de la dématérialisation des appels d'offres, le risque est réel. Il n'y a pas de raisons que les attaques que le secteur privé subit tous les jours ne soient pas transposées dans le secteur public.
Qu'est ce qui empêchera demain une entreprise d'aller voir l'offre faite par ses concurrents dans le cadre d'un appel d'offre ? Qui pourra empêcher une personne mal intentionnée de diffuser des informations confidentielles collectées illégalement auprès d'une collectivité ?

Quels sont les points à améliorer d'urgence ?

Il s'agit avant tout de créer une culture de la sécurité des systèmes d'information à tous les niveaux et donc de former tout le personnel. Pour cela, les élus doivent être moteurs.
Dans un premier temps, des choses très simples peuvent êtres mises en œuvre comme, ne pas laisser le mot de passe sur un post-it sur l'écran du PC ou ne pas se débarrasser de ses anciens ordinateurs sans s'être au préalable assuré qu'il n'y ait plus de données dessus !

Le niveau des protections est-il vraiment si faible ?

Malheureusement oui. Plus de 65 % des collectivités interrogées n'ont pas de responsable informatique et les trois quarts n'ont pas de budget dédié à la sécurité de leurs systèmes d'information. Sans parler de malveillance, la simple sécurisation des données est déjà très problématique. Plus de 60 % des collectivités interrogées ne les externalisent pas. En cas d'incendie ou d'inondations, elles peuvent alors tout perdre et ne plus êtres capables de fonctionner correctement.

Que faut-il mettre en place pour sauvegarder efficacement des données ?

Il faut absolument qu'elles soient sauvegardées sur deux lieux différents, et pas simplement deux pièces d'une mairie ! Par exemple, il s'agit de déposer régulièrement ces données à la banque ou de faire appel à un prestataire extérieur. Dans ce cas, il s'agit de bien s'assurer de la fiabilité de ce prestataire. Par exemple, vérifier qu'il ne stockera pas les informations dans le cloud, qui n'est pas forcément le lieu le plus sécurisé !

Et pour se prémunir des attaques existe-t-il une recette ?

Du bons sens avant tout. 80 % des problèmes sont évitables avec de simples mesures de bon sens. Pour aider les collectivités à mieux se protéger, l'Etat a publié un très bon référentiel général de sécurité des systèmes d'informations .
Malheureusement, il ressort du sondage que les trois quarts des collectivités ne connaissent pas ce document et qu'à même proportion elles ne connaissent pas jusqu'à l'existence de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) qui est pourtant l'agence de référence. C'est toute une nouvelle culture qu'il faut aujourd'hui créer autour de ces nouveaux risques.

Les collectivités ont des pratiques inégales en sécurité informatique

Publié le 18/03/2013

La politique de sécurité informatique des collectivités ne peut que progresser. L'utilisation des outils personnels et la mobilité des agents devraient être des points de vigilance.

Moins d'un tiers des collectivités (31 %) ont adopté **une politique de sécurité informatique**, selon une étude du Club de la sécurité de l'information français (Clusif)*. Pourtant, plus de deux sur trois (68 %) reconnaissent que leurs activités dépendent fortement de l'informatique, poussées notamment par l'évolution de l'e-administration : téléprocédures, dématérialisation des marchés publics...

Les structures intercommunales, plus jeunes, et les villes moyennes, se préoccupent moins de la sécurité informatique que les conseils généraux, conseils régionaux et grandes villes. Sans doute par manque de moyens et par ignorance.

Principal frein à la conduite des missions de sécurité : l'absence de personnel qualifié (33 %). Viennent ensuite (27 % pour chacun) le manque de connaissances et les moyens financiers contraints, ce qui représente une différence notable avec la précédente enquête du Clusif : en 2008, le manque de budget était la principale raison invoquée. Les budgets consacrés à la sécurité de l'information sont toutefois variables en fonction de la taille des collectivités.

Sensibiliser les agents

Le Clusif note que 62 % des collectivités seulement appuient leur politique de sécurité sur des référentiels et qu'elles ne sont que 32 % à avoir désigné un responsable de la sécurité des systèmes d'information (RSSI ou RSI). Une collectivité sur trois (33 %) adopte une démarche formelle d'analyse des risques au moins partielle, chiffre en diminution par rapport à 2008.

La sensibilisation des utilisateurs à la sécurité n'a pas progressé. Seules 29 % des collectivités ont lancé ou préparent des actions de sensibilisation, alors que les agents sont de plus en plus nombreux à utiliser leurs outils informatiques personnels sur les lieux de travail, renforçant la vulnérabilité du système d'information.

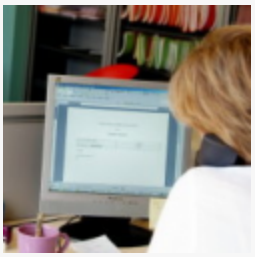
Les experts du Clusif estiment que ce phénomène du "Byod" (Buy Your Own Device) devrait inciter les collectivités **à communiquer sur la sécurité auprès de leurs agents**, notamment - mais pas uniquement - par **la formalisation de chartes informatiques**.

Un autre point à surveiller est la mobilité des agents au sein des collectivités. La direction des systèmes d'information (DSI) n'est pas systématiquement informée des départs ou des mutations. Or, ces mouvements de personnel devraient entraîner la clôture de leurs droits d'accès au réseau de la collectivité et la restitution de tout le matériel informatique.

La rigueur budgétaire aura probablement un impact sur la sécurité des systèmes d'information. Rationaliser les dépenses impliquera de concentrer les moyens sur les points les plus sensibles. Pour cela, les collectivités devront procéder à des analyses de risques informatiques plus élaborées.

INFO MAIRES le guide

LA PRÉVENTION DES RISQUES INFORMATIQUES



La sécurité informatique est une des préoccupations majeures des services techniques de la commune à l'heure où la dématérialisation est en marche et augmente les échanges de données informatiques. Pour y répondre au mieux, certaines collectivités ont fait le choix de solutions informatiques novatrices.

Des solutions informatiques de gestion financière et de ressources humaines intégrées, ergonomiques et souples d'utilisation, adaptées à la taille de la collectivité, une technologie full web qui favorise les échanges et la communication entre domaines applicatifs en répondant parfaitement aux exigences de performance et de sécurité, tels sont les choix de progiciels informatiques mis en place par ces collectivités.

La sécurité informatique en est renforcée !

Ce qui peut arriver

Un système informatique compliqué et éparpillé sur plusieurs sites, une panne informatique du serveur hébergeant tout ou partie du réseau informatique mis en place dans la collectivité ; une panne de courant ; la prolifération des virus informatiques, une catastrophe naturelle entraînant la destruction partielle ou complète des installations informatiques ou encore, des actes de vandalisme, … les risques liés à la mise hors d'état de fonctionner du système d'information dans une collectivité territoriale sont nombreux.

Principe de fonctionnement du modèle Saas

SaaS (Software as a Service) : cet acronyme désigne une opportunité bien réelle pour tous les utilisateurs d'applications informatiques, à savoir la possibilité d'accéder à distance et à la demande à l'ensemble des logiciels* de gestion, via un navigateur, sans avoir à administrer les différents composants nécessaires à leur utilisation.

La solution se consomme ainsi "comme un service" via un abonnement périodique.

Quels avantages pour la collectivité ?

Le SaaS apporte au moins 3 réponses concrètes aux impératifs des responsables des collectivités et administrations.

La première concerne leur capacité à anticiper la diminution de ressources, qui impliquera l'ensemble des services. Dans ce contexte, la possibilité de maîtriser les effectifs techniques, internes et externes, apparaît comme une marge de manœuvre particulièrement bienvenue.

Le deuxième apport du mode SaaS est, dans le même esprit que le premier, de permettre de libérer les agents de nombreuses tâches chronophages, telles que l'administration, la maintenance applicative, les mises à jour ou une bonne part du support aux utilisateurs.

Le troisième aspect porte sur les qualités techniques des solutions disponibles, tant sur le plan de la sécurité du système mis en place que de la protection des données.

Services d'exploitation et maintenance applicative

- Double sauvegarde des données
- Procédures de restauration automatiques
- Gestion et planification des changements de versions : Système d'exploitation, Bases de données, anti-virus…
- Mise à jour automatique des versions et des patchs des applications de gestion
- Assistance hotline
- Veille et mise à jour réglementaire

Sécurité & pilotage

- Sécurité optimale, via pare feux et antivirus
- Contrôles d'accès et vidéo surveillance des sites d'hébergement 24h/24 - 7j/7
- Surveillance des serveurs et du réseau
- Protocole d'alertes
- Confidentialité
- Surveillance applicative

Une sécurité informatique optimisée à moindre coût pour la collectivité

- Des investissements informatiques planifiés et maîtrisés (via un forfait périodique)
- Un déploiement souple et immédiat
- Un système d'information optimisé et sécurisé
- Une accessibilité à la solution ‘partout, à tout instant'
- Une intégration des évolutions métier et technologiques en toute transparence
- Un engagement clair de la part de votre partenaire informatique (Contrat SLA*), portant sur la qualité du service apporté, la disponibilité, la performance et la réactivité.

(*Service Level Agreement : engagement de service)

Définition

Logiciel : un logiciel ou une application est un ensemble de programmes, qui permet à un ordinateur ou à un système informatique d'assurer une ou plusieurs tâche (s) et/ou fonction (s), par exemple, logiciel de gestion de la paie, logiciel de traitement de texte, logiciel de comptabilité.

En savoir plus

http://www.cegid.fr/secteurpublic, rubrique : choisir le mode SaaS.

Agence Nationale de la Sécurité des Systèmes d'information

Portail de la Sécurité informatique
http://www.securite-informatique.gouv.fr

Mémentos > Archivage électronique sécurisé

Contexte et enjeux de l'archivage électronique sécurisé

Contexte et enjeux de l'archivage électronique sécurisé

Avant la mise en place effective d'un archivage électronique sécurisé, il est indispensable de s'interroger sur l'existant en matière d'archivage électronique en tenant compte du contexte à la fois technique et juridique. Cette étude préalable doit permettre de déterminer et d'apprécier les enjeux de l'archivage électronique sécurisé, en identifiant les besoins et les contraintes générales à prendre en compte dans une approche nécessairement pluridimensionnelle.

Architecture de l'archivage électronique

L'architecture de l'archivage électronique doit être envisagée selon deux axes indissociables en la matière : les aspects juridiques et opérationnels (technique et sécurité).

La partie juridique est le fruit d'une approche pratique et pluridimensionnelle. Elle a pour objectif de faciliter l'appréhension de la relation étroite qui existe entre le juridique et le technique en matière d'archivage électronique. Ainsi, doivent être présentés et hiérarchisés, les textes et travaux qui ont trait au concept d'archivage électronique et plus largement à la dématérialisation (valeur probante, signature électronique, factures électroniques, marchés publics dématérialisés...). Cette approche vise à préciser la portée, l'intérêt et/ou les implications que chacun d'entre eux est susceptible d'avoir sur l'archivage électronique.

Ce référentiel établi, le périmètre technique et opérationnel d'un service global d'archivage électronique et plus précisément d'un système d'archivage électronique (SAE) doit être appréhendé. Avant d'entrer dans le détail de l'architecture, il est nécessaire d'aborder les contraintes techniques, puis les différentes organisations possibles pour un service d'archivage en s'appuyant sur les normes actuelles en la matière. Ensuite, le détail des fonctionnalités d'un SAE doit être déterminé en prenant en compte la sécurité logique et physique du système. Enfin, les décideurs doivent prendre en compte les offres en matière de logiciels et services puis analyser les coûts afin de pouvoir comparer différentes solutions. Les développements qui suivent présentent de façon synthétique le contenu de ces différentes phases.

les contraintes techniques

En matière de contraintes, les notions de formats logiques doivent être prises en compte, c'est-à-dire sous quelle forme va se présenter une information à archiver. Par exemple, s'agit-il d'un texte ou d'une image ?Le format XML est largement recommandé de part compte son aspect de standard ouvert et extensible mais aussi en tant que métalangage.

Les formats physiques ou différents types de supports utilisables auxquels s'ajoute la notion de WORM (*Write Once Read Many*) doivent également être appréhendés. Le WORM peut être vu comme une référence à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable Une distinction est d'ailleurs faite entre WORM physique et WORM logique résultant dans la manière de gérer les propriétés évoquées précédemment en ayant recours ou non à une transformation irréversible du substrat. Il en va de même des supports magnétiques (bandes et disques) et des supports optiques (CD, DVD) sachant que le choix se fera en fonction des exigences, comme la stabilité de ces supports ou encore leur large diffusion.

Une autre contrainte est celle des accès au système qui se doivent d'être performants quelle que soit la volumétrie à traiter. Cette dimension est à prendre en compte le plus en amont possible.

Les problèmes de migration auxquels tout archivage électronique se verra confronté constituent un paramètre et un enjeu primordiaux. L'évolutivité du système constitue également une des composantes de l'archivage électronique, d'autant qu'elle devra pouvoir se faire sans impact significatif sur la qualité du service rendu. Les aspects sécurité, outre la sauvegarde des informations archivées, sont à prendre en compte et induisent la notion de traçabilité de l'ensemble des opérations et évènements survenus au sein du système. Enfin, la prise en compte de la signature électronique se doit d'être soulignée afin de bien définir les contraintes afférentes.

les différentes organisations

Au niveau organisationnel, les différents modèles et normes existants en matière d'archivage doivent servir la réflexion

en tenant compte de leurs champs d'application, principaux avantages et inconvénients. Il en est ainsi du modèle OAIS (*Open Archival Information System*) come de la norme NF Z42-013 en passant par la norme ISO 15489 ou autre modèle MOREQ (*Model requirements for the management of electronic records*).

C'est à l'issue de cette étude que l'architecture d'un service d'archivage électronique pourra pleinement être élaborée.

Il s'ensuit que les grandes fonctions d'un archivage électronique sécurisé et d'un système d'archivage électronique, doivent être : - le versement, - le stockage, - la gestion des données descriptives, - la consultation/communication - et une dernière et cinquième fonction : l'administration au sens large y compris la gestion de la relation avec les services producteurs, la veille technologique et juridique ou encore les projets d'évolution et de migration.

La sécurité d'un système d'archivage

En matière de sécurité, l'administration générale et l'organisation, les aspects physiques, la sécurité des locaux, les contrôles d'accès des personnels aux bâtiments et aux différents matériels, la sécurité des personnels, du matériel et du logiciel sont également des aspects indispensables à prendre en considération.

Ceci étant, le SAE doit aussi reposer sur des règles de sécurité spécifiques mais qui viennent s'ajouter à celles définies à titre général dans la politique d'archivage électronique sécurisé et dans la politique de sécurité des systèmes d'information si cette dernière existe. À ce titre, le SAE qui est un système d'information doté d'une finalité particulière doit intégrer une analyse des risques tout au long du processus d'archivage.

Les logiciels d'archivage

En ce qui concerne les offres logiciels, le marché propose aujourd'hui un panel assez large et diversifié de solutions d'archivage qui se précise et se complète d'année en année. La typologie des produits va du coffre-fort à la solution générale qui englobe l'archivage dans la gestion du cycle de vie complet des données (ILM).

Les produits du marché mettent tantôt l'accent sur la gestion de contenu, tantôt sur l'archivage légal (l'expression est répandue mais il serait plus exact de dire « archivage à des fins de preuve »). Ils visent soit l'ensemble des données d'une organisation (incluant parfois les données sur les archives papier), soit un type d'information ou un format de document bien spécifique, tel que les messages électroniques.

Dans le secteur technique et scientifique, existent également des offres notamment en terme d'infrastructures de stockage (très grandes volumétries) et d'outils performants d'accès et de consultation des données archivées. En revanche, il existe encore très peu de briques logicielles prenant notamment en compte la partie gestion des versements sur la plateforme d'archivage suivant un format donné, le contrôle des formats, leur conversion éventuelle..., ainsi que l'alimentation automatique d'une base de données descriptive à partir notamment des métadonnées des objets archivés accompagnant le versement.

Au niveau logiciel, il faut également choisir entre une solution du marché, un logiciel libre ou encore un développement spécifique. L'essentiel est de bien prendre la mesure de ses choix, étant entendu que les changements de politique auront un coût qu'il vaut mieux connaître à l'avance et si possible éviter ou, à tout le moins, anticiper. Il est également important de considérer les questions techniques de récupération des données et de maintenance.

Les autres critères importants de l'archivage sécurisé

En complément à l'offre logiciel, un certain nombre de critères à analyser et à vérifier dans le processus de choix d'une solution doit être retenu, à savoir : l'interopérabilité et le partage de ressources, critères très importants pour la pérennité du service et sa continuité, la facilité de prise en compte des données descriptives pour les consultations ultérieures, les temps et les contrôles d'accès, la montée en charge tant pour les accès que pour la volumétrie, le stockage de sorte qu'il corresponde bien aux besoins et aux souhaits de l'organisation (*on line, off line, near line*), la prise en compte des possibilités de migrations tant de supports que de format, l'évolutivité sous les aspects à la fois des volumes et des accès mais également la capacité à changer de système facilement en tout ou partie, le coût direct du logiciel et les coûts associés du type support et maintenance, la pérennité du fournisseur/éditeur.

En ce qui concerne les coûts la réflexion et l'approche doivent essentiellement permettre de choisir une solution parmi d'autres. Dans ce cadre, le fait de répertorier l'ensemble des coûts de façon exhaustive, tant en matière d'investissement direct (matériel informatique, réseau, sécurité, prestations...) qu'en exploitation (télécommunications, locaux, personnel, maintenance...) ou autres coûts comme les consommables, apparaît comme une opération délicate qu'il conviendra de mener avec rigueur.

Le système de simulation

À partir du moment où le décisionnaire dispose de l'ensemble des données, il s'agit de mettre en place une véritable simulation du fonctionnement du système d'archivage, en terme de coûts et pour une période donnée. L'avantage de disposer d'un système de simulation est avant tout de permettre la prise en compte à la fois des coûts ponctuels et des coûts récurrents et éventuellement de pouvoir analyser la sensibilité des paramètres identifiés.

Enjeux juridiques de l'archivage électronique

Le contexte et les enjeux juridiques de l'archivage électronique doivent être appréhendés eu égard aux textes et concepts juridiques qui s'imposent en matière d'archivage.

Dresser le panorama juridique de l'archivage électronique sécurisé conduit à prendre en compte le régime juridique applicable aux archives électroniques afin qu'elles conservent la valeur juridique que l'acte recouvrait lors de son établissement. En ce sens, il s'agit :

- d'identifier les exigences juridiques que l'archivage électronique devait garantir dans le temps, c'est-à-dire dans le cadre de l'archivage, jusqu'à la fin de la durée de conservation nécessaire (qui soit est imposée par un texte, soit est déterminée à des fins de preuve).
- prendre en compte les modalités de l'archivage électronique qui trouvent à s'imposer au-delà de l'objet archivé et qui portent directement sur les obligations et responsabilités des différents acteurs de l'archivage.

Une analyse des aspects juridiques conduit à considérer que :

* Il n'existe pas de cadre juridique spécifique à l'archivage électronique : il est donc nécessaire de partir des principes juridiques généraux qui trouvent à s'appliquer pour en apprécier la portée dans le contexte de l'archivage électronique ;

* Un acte électronique n'ayant aucune valeur juridique lors de son établissement ne pourra se voir conférer une telle valeur au seul motif qu'il a été archivé électroniquement. En revanche, un acte doté d'une valeur juridique peut la perdre au motif qu'il a été conservé dans de mauvaises conditions. C'est pourquoi, seul un « archivage électronique sécurisé » permettra au juge d'apprécier la valeur juridique du document conservé, la conservation réalisée devant répondre aux exigences légales ou jurisprudentielles et conditionnant le fait que cet acte produise des effets juridiques.

Cette approche conduit à donner la définition suivante de l'archivage électronique sécurisé : l'ensemble des modalités de conservation et de gestion des archives électroniques ayant une valeur juridique lors de leur établissement ; cet archivage garantissant la valeur juridique jusqu'au terme du délai durant lequel des droits y afférents peuvent exister.

Cette définition est déterminée au vu des principes juridiques impactant l'archivage électronique sécurisé et des obligations et responsabilités qui en découlent pour les personnes intervenant en la matière.

Principes juridiques directeurs impactant l'archivage électronique sécurisé dans la sphère privée

Les principes directeurs de l'archivage électronique dans la sphère privée permettent de mettre en exergue :

- la nécessité d'identifier le domaine juridique dans lequel s'inscrit le document. Durée de conservation, finalité (validité, preuve...), formalisme connexe (LRAR, double exemplaire...) sont autant de paramètres à prendre en compte pour définir les bonnes modalités d'archivage ;

- lorsque l'identification de l'auteur ou de l'origine de l'acte fait partie intégrante de sa valeur juridique, l'archivage électronique doit prendre en compte et traiter l'ensemble des éléments participant à l'imputabilité de l'acte conservé (signature électronique, certificat...) ;

- les écrits électroniques (à titre de preuve, de validité, qu'il s'agisse de contrat ou facture par exemple) doivent être conservés de telle sorte que leur intégrité soit garantie. L'archivage électronique devra respecter cette exigence commune à la reconnaissance juridique des écrits électroniques en droit privé ;

- l'archivage électronique représente un enjeu majeur : si la conservation ne garantit pas les conditions exigées pour la reconnaissance d'un écrit électronique et remplies à la date de son établissement, l'écrit électronique perd sa valeur juridique ;

- les conditions d'intelligibilité, d'imputabilité, d'intégrité et de respect de formalités parfois connexes (type LRAR) doivent être garanties dans le cadre d'un archivage électronique à des fins juridiques. L'archivage doit les garantir dans le temps. Ainsi, le contenu informationnel doit être maintenu dans son intégrité mais pas forcément dans les mêmes formes et sur les mêmes supports. Mais, comment allier l'évolution des technologies qui a une incidence directe sur l'intelligibilité des actes avec la garantie d'intégrité dans le temps ? C'est là la problématique majeure de l'archivage électronique.

en tout état de cause, l'archivage électronique doit reposer sur une traçabilité des documents et des opérations afférentes. Elle doit être garantie aux différentes phases concernées et dépasse la question des supports utilisés.

Principes juridiques directeurs impactant l'archivage électronique sécurisé dans la sphère publique

Il est certain que dans le cadre de l'archivage d'actes électroniques, l'archivage effectué devra porter sur l'ensemble des éléments permettant d'apprécier la légalité et/ou la valeur probante de cet acte. En ce sens, pour que l'archivage remplisse sa finalité juridique, il faudra que les modalités mises en place permettent de garantir les conditions imposées pour la reconnaissance juridique des documents eux-mêmes.

Dans le cadre d'un archivage électronique dans une finalité juridique, le juge administratif pourra être convaincu de la valeur juridique du document archivé aux conditions cumulatives que :

- l'acte soit intelligible par lui ;

- l'auteur du document électronique puisse être dûment identifié (garantie de la compétence juridique de l'auteur de l'acte) ;

- le document ait été établi et conservé dans des conditions de nature à en garantir l'intégrité (toute altération ou modification du document doit être détectable, à défaut le juge pourra douter de la fiabilité de l'écrit électronique et donc de sa valeur juridique, que ce soit à titre de preuve ou de légalité).

De plus, pour que l'archivage électronique soit regardé comme fiable d'un point de vue juridique, il apparaît nécessaire que les procédures mises en place soient précisément décrites et mises en œuvre (il en va ainsi des métadonnées qui font à ce titre l'objet d'un standard d'échange). L'automatisme de certaines opérations dont la datation des versements constitue en ce sens une sécurité. De même, il pourrait être envisagé qu'un certain nombre de documents soit scellé à la date de leur versement aux archives. De la sorte, si les administrations ont la maîtrise de l'archivage de leurs documents, elles en garantissent l'efficacité et la fiabilité du fait de processus externes (logiciels...) dont elles n'ont pas la maîtrise.

D'une façon générale, l'ensemble des opérations devra être tracé. A cet effet des procédures devront être définies en tenant compte des prescriptions applicables à l'archivage en général (DUA, bordereau de versement, opération de tri, bordereau d'élimination...) et des règles relatives à la consultation et à la communication des documents archivés (accès réservé, liberté de communication...).

Enfin, s'il n'existe pas de règles juridiques spécifiques à l'archivage électronique, il est nécessaire de prendre en compte les règles de droit commun applicables à l'archivage papier, en adaptant les modalités de l'archivage électronique afin de préserver les spécificités liées à la nature électronique des documents. De même, la question des formats et des supports utilisés doit faire l'objet d'une réflexion adéquate en fonction de la nature des archives et de la durée de conservation fixée. La problématique de la migration des documents constitue là encore un des enjeux majeurs de l'archivage électronique à des fins juridiques. Et les observations faites à cet égard en droit privé se retrouvent de façon similaire.

Obligations juridiques et recommandations subséquentes en matière d'archivage électronique

Quel que soit l'acteur en cause (sphère publique / sphère privée), un ensemble d'obligations techniques, organisationnelles et juridiques conditionne la mise en place d'un archivage électronique sécurisé et sa fiabilité afin de conserver la valeur juridique aux archives électroniques traitées. Parmi ces obligations, certaines sont générales, d'autres propres à l'environnement numérique (atteinte aux STAD, traitement de données à caractère personnel, données de connexion...) ou propres à la sphère publique. L'on peut ainsi distinguer :

- les obligations générales à respecter compte tenu des exigences juridiques, notamment :

* Le respect des durées de conservation imposées par les textes. Il sera ainsi nécessaire de déterminer la durée de conservation de l'archive en cause qui est fonction de son régime juridique. Un travail en amont permettant d'établir une typologie des différentes durées de conservation est alors indispensable. A cet égard, pour les archives privées, il conviendra de se conférer aux différents textes juridiques dont l'acte relève ; pour les archives publiques, les durées d'utilité administrative fixées par les services compétents devront être pris en compte ; * Le respect du secret professionnel : cette obligation est clairement imposée pour les archives publiques et privées qui ne peuvent être mises à la disposition du public. En cas de manquement, des sanctions pénales sont encourues. * Le respect de la confidentialité des correspondances : dans la mesure où les correspondances constituent des archives, les principes applicables en la matière doivent être respectés même lorsqu'elles sont sous forme électronique.

- les obligations spécifiques à l'environnement numérique :

* L'obligation de sécurité en vue d'éviter les atteintes aux Systèmes de Traitement Automatisé de Données. Cette obligation nécessite de prévoir les procédures et moyens à mettre en place à titre préventif, réactif et répressif le cas échéant. Le lien avec la Politique de sécurité des systèmes d'information, si elle existe, est ici primordial ;

* Les obligations de protection relatives aux traitements de données à caractère personnel ; * Le respect de la législation en matière de cryptologie.

- les obligations spécifiques aux archives publiques :

* Les obligations dont le non respect est constitutif d'infractions spécifiques ; Les obligations tenant à la gestion des archives publiques notamment en ce qui concerne les modalités de versement, de communication, d'élimination ou de contrôle des archives publiques. À ce titre, il convient donc de prendre en compte et de transposer les formalités et procédures requises pour le papier et de les adapter (exemple : lieu du « dépôt », lieu d'hébergement de la plateforme d'archivage électronique...) ; * L'exclusion de principe du recours à un tiers archiviste.

L'analyse de ces obligations met en avant certaines recommandations valables en tout état de cause :

- assurer la traçabilité de toutes les opérations concernant les archives versées (communication, migration, éventuelle élimination...) ; - veiller à l'interopérabilité des systèmes d'archivage ; - suivre l'état de l'art pour les migrations ; - établir et mettre en œuvre une politique d'archivage électronique visant à définir les rôles de chaque intervenant dans le processus d'archivage électronique (service versant, autorité d'archivage, contrôleurs...), les obligations et

responsabilités y afférent ; - procéder ou faire procéder aux audits adéquats.

En pratique, les obligations précitées ont des implications fonctionnelles et opérationnelles qui se retrouvent à chacune des phases de l'archivage (versement, stockage, tri, élimination, administration, accès, communication....).

C'est pour cette raison que l'identification préalable des rôles de chaque intervenant est fondamentale. A cet égard, alors qu'il existe une grande liberté organisationnelle et structurelle dans la sphère privée, il convient de constater que les procédures dans la sphère publique sont strictement encadrées (procédures de versement, procédures de tri, procédures d'élimination, procédures de communication...). Ceci d'autant plus que les responsabilités dans la sphère publique sont étroitement liées aux règles organisationnelles imposées par le code du patrimoine et le code général des collectivités territoriales.

Il en va ainsi du recours à des tiers archivistes qui est prohibé pour les archives publiques (sauf deux exceptions dont le fondement juridique reste fragile) alors qu'il permet aux personnes privées de transférer contractuellement la charge de certaines obligations et donc de limiter leur responsabilité en interne.

Régimes de responsabilité

Les régimes de responsabilité sont très différents selon qu'il s'agisse d'une personne privée ou d'une personne publique. Partant de ce préalable, les régimes de responsabilités doivent être appréhendés distinctement pour chacun de ces acteurs et suivant les modalités pouvant être retenues pour effectuer cet archivage électronique.

Ainsi, dans la sphère privée, ce sont les principes de la responsabilité civile qui sont applicables tant pour les personnes morales que pour les salariés (étant noté les effets juridiques des délégations) et les liens contractuels qui peuvent exister avec des prestataires externes.

Pour les archives publiques, c'est le régime de responsabilité administrative qui s'applique pour les personnes morales concernées (personnes publiques, personnes privées chargées d'une mission de service public) et les agents (régime de la faute / droit disciplinaire).

La responsabilité pénale est également un des aspects à prendre en compte.

****

Cette première démarche, nécessaire en amont de tout projet, permet d'identifier concrètement les enjeux et le contexte de l'archivage électronique sécurisé. La définition des besoins, l'identification de l'existant, des moyens, des exigences et du contexte doivent précéder puis accompagner la mise en place opérationnelle de l'archivage électronique sécurisé.

L'analyse du contexte et des enjeux de l'archivage électronique sécurisé permet également de relever que, si des points de similitude existent, qu'il s'agisse d'archives électroniques publiques ou privées, les points de divergence entre les deux sphères commandent de traiter distinctement les documents à adopter pour organiser l'archivage électronique sécurisé.

En effet, alors que les acteurs privés bénéficient d'une certaine souplesse quant aux modalités organisationnelles de leurs archives, l'organisation des archives publiques est strictement encadrée (notamment par le code du patrimoine et les textes réglementaires).

De plus, la spécificité de l'organisation dans la sphère publique a des implications directes sur les modalités de mise en place de l'archivage électronique et sur son architecture, compte tenu des rôles des différents intervenants tant d'un point de vue fonctionnel que juridique.

Les aspects opérationnels doivent tenir compte de ces divergences.

CNIL.

Fiche pratique

10 conseils pour la sécurité de votre système d'information

12 octobre 2009

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support. La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois). Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2...), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « génériques » ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum) ; les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné. Par ailleurs, le contrôle de l'usage des ports USB sur les postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en terme de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance. Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données qui peuvent être considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.

Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des

Lexique :

Profil d'habilitation : un profil d'habilitation définit, pour un groupe d'utilisateurs, leurs droits sur un ensemble de données et/ou d'applications.

Routeur filtrant et ACL : un routeur est un équipement qui permet l'aiguillage de l'information entre deux réseaux. Certains routeurs intègrent une fonction de filtrage du trafic, telle que celle des pare-feu, qui met en œuvre une liste des adresses et ports autorisés ou interdits d'accès (Access Control List).

Pare-feu (ou « firewall ») : équipement logiciel et/ou matériel permettant de cloisonner des réseaux. Il met en œuvre des règles de filtrage du trafic entrant et sortant et doit interdire l'utilisation de protocoles de communication non sécurisés (Telnet par exemple).

« tunneling » ou VPN (réseau privé virtuel) : un VPN permet de sécuriser les échanges de données de type "extranet". Pour cela, il met en œuvre un mécanisme d'authentification et de chiffrement des données. On parle alors d'encapsulation des données grâce à un protocole de « tunneling ».

Chiffrement : méthode de codage/décodage des données mettant généralement en œuvre un mécanisme de clé(s) logique(s) afin de rendre impossible la lecture d'un fichier à des tiers qui ne possèdent pas la ou les clé(s).

IPsec, SSL/TLS, HTTPS : protocoles réseaux permettant de sécuriser les accès distants par chiffrement des données transmises.

Tolérance de panne : dispositif de sécurité mis en œuvre notamment au niveau des disques durs qui permet de se prémunir de la panne d'un disque en évitant l'arrêt des applications ou l'endommagement des données stockées.

BIOS : système exécutant, à la mise sous tension d'un ordinateur, des opérations élémentaires telles que le contrôle des éléments matériels, l'ordonnancement de démarrage des périphériques, la lecture d'un secteur sur un disque.

routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents. La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière. Les connexions entre les sites parfois distants d'une entreprise ou d'une collectivité locale doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel). Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc. Enfin, les accès distants au système d'information par les postes nomades doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

« A noter » : Un référentiel général de sécurité, relatif aux échanges électroniques entre les usagers et les autorités administratives (ordonnance 2005-1516), doit voir le jour prochainement (voir projet sur le site www.ssi.gouv.fr). Il imposera à chacun des acteurs des mesures de sécurité spécifiques.

7. Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé. Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur. Les supports nomades (ordinateurs portables, clé USB, assistants personnels etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information. Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable, du service juridique ou du CIL de l'entreprise ou de l'organisme dans lequel il travaille.

Ce document doit s'accompagner d'un engagement de responsabilité à signer par chaque utilisateur.

A noter : veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes. De même, nettoyer régulièrement le répertoire d'échange partagé entre les différents services afin qu'il ne se transforme pas en espace « fourre-tout » (fichiers personnels des agents mélangés avec des dossiers sensibles)

Le référentiel général de sécurité (RGS)

L'ADMINISTRATION ÉLECTRONIQUE EN TOUTE CONFIANCE

Le développement de l'administration électronique est l'un des principaux leviers de l'amélioration de la qualité des services publics. Pour permettre cet essor, la confiance des usagers est primordiale. Dans le monde des échanges numériques, la confiance se construit pour une large part en garantissant la sécurité des systèmes d'information.

C'est pour répondre à cet enjeu et aider les autorités administratives à y faire face qu'a été élaboré le référentiel général de sécurité (RGS).

1. Qu'est-ce que le RGS ?

Le RGS est un recueil de règles et de bonnes pratiques en matière de sécurité des systèmes d'information destiné principalement aux autorités administratives qui proposent des services en ligne aux usagers.

Des bonnes pratiques de gestion de la sécurité des systèmes d'information

Le RGS encourage les administrations à adopter une approche globale pour la protection de leurs systèmes d'information afin de mettre en œuvre des mesures de sécurité cohérentes, adaptées aux enjeux et répondant aux besoins de sécurité. Ceci passe par une **analyse systématique des risques** qui pèsent sur les systèmes d'information. Cette analyse, qu'il est souhaitable de faire dès la phase amont des projets, est régulièrement mise à jour pour permettre une **amélioration continue** de la sécurité des systèmes d'information.

Des règles techniques concrètes

Selon les fonctions de sécurité (cf. encadré ci-contre) retenues et le niveau de sécurité souhaité par l'autorité administrative, le RGS définit les exigences techniques et les moyens de protection pertinents en termes de produits de sécurité et d'offres de services de confiance. **Le RGS constitue ainsi un cadre adaptable aux enjeux et aux besoins spécifiques de chaque autorité administrative.**

Quatre fonctions de sécurité

- **L'authentification :**
l'authentification est l'action par laquelle le système d'information vérifie l'identité de l'usager. Les procédés utilisés par l'usager pour prouver son identité vont de l'emploi d'un couple identifiant/mot de passe à l'utilisation d'un certificat électronique personnel stocké sur une carte à puce.

- **La signature électronique :**
la signature d'un document électronique garantit l'identité du signataire et l'intégrité du document signé.

- **La confidentialité :**
cette fonction permet de s'assurer qu'une information ne peut être consultée par un tiers non autorisé au cours de son transfert ou de son stockage.

- **L'horodatage :**
ce procédé permet de garantir qu'un document ou un message existait à un instant donné. Il fait foi dans le domaine des échanges électroniques.

2. Les objectifs du RGS

Le RGS a pour principal objectif de développer la confiance des usagers et des administrations dans leurs échanges numériques.

Dans ce cadre, le RGS permet notamment :
• de favoriser l'adoption par les administrations de bonnes pratiques en matière de sécurité des systèmes d'information ;
• d'adapter les solutions techniques aux justes besoins de sécurité identifiés pour chaque système d'information ;
• d'offrir aux autorités administratives les labels de sécurité permettant de s'assurer de la qualité des produits et des services de sécurité proposés par le marché ;
• de favoriser le respect des dispositions de la loi « informatique et libertés » relative à la protection des données personnelles.

Quel est le cadre juridique du RGS ?
• Le RGS est prévu par l'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Cette ordonnance définit le périmètre et le rôle du référentiel général de sécurité : « fixer les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique ».
• Le décret n° 2010-112 du 2 février 2010 porte création du référentiel général de sécurité.

3. À qui s'adresse le RGS ?

Le RGS s'adresse avant tout aux autorités administratives. Il s'adresse également aux prestataires qui les assistent dans la sécurisation des échanges dématérialisés.
Les directeurs de services informatiques, les responsables de la sécurité des systèmes d'information de même que les chefs de projets au sein de maîtrises d'œuvre sont les principaux acteurs pour lesquels le RGS est utile.
Le RGS est également destiné aux :
• prestataires de services de confiance (par exemple, les fournisseurs de certificats électroniques) ;
• industriels développant des produits de sécurité.

De qui émane le RGS ?
Le RGS est le résultat d'un travail conjoint entre l'agence nationale de la sécurité des systèmes d'information (ANSSI) et la direction générale de la modernisation de l'État (DGME).

Qu'est-ce que l'ANSSI ?
L'agence nationale de la sécurité des systèmes d'information, service du Premier ministre, est rattachée au secrétaire général de la défense et de la sécurité nationale. Créée le 7 juillet 2009, elle est l'autorité nationale en matière de cybersécurité.

Plus d'informations sur le RGS :

www.references.modernisation.gouv.fr

Rendez-vous sur le site pour :
• obtenir les documents constitutifs du référentiel ;
• télécharger les supports méthodologiques pour sa mise en œuvre ;
• connaître l'actualité du RGS.

Retrouvez également sur ce site les documents de référence de l'administration électronique sur l'accessibilité, l'interopérabilité et l'ergonomie des sites Internet publics.

Contact:
•DGME - Service Projets : rgs.dgme@finances.gouv.fr
•ANSSI (pour les questions techniques) : rgs@ssi.gouv.fr

LA DIRECTION GÉNÉRALE DE LA MODERNISATION DE L'ÉTAT

Au sein du ministère du Budget, des Comptes publics et de la Réforme de l'État, la direction générale de la modernisation de l'État (DGME) pilote le suivi de la mise en œuvre de la révision générale des politiques publiques et accompagne les ministères dans leurs chantiers de transformation. À l'écoute des usagers et de leurs attentes, la DGME conduit également des chantiers interministériels structurants dans les domaines de l'administration électronique, de la simplification administrative, de l'amélioration de l'accueil des usagers et de la qualité des services publics.

Conception graphique : Agasic

DIRECTION DES AFFAIRES JURIDIQUES

LE REFERENTIEL GENERAL DE SECURITE – RGS ET LES CERTIFICATS DE SIGNATURE ELECTRONIQUE DANS LES MARCHES PUBLICS

INFORMATIONS PRATIQUES APRÈS L'ECHEANCE DU 19 MAI 2013

I / Le RGS

Le référentiel général de sécurité prévu par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005[1] fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

L'article 14 de l'ordonnance fixe le calendrier qui s'impose aux autorités administratives pour la mise en conformité de leurs systèmes d'information avec le RGS : « *Les systèmes d'information existant à la date de publication du référentiel général de sécurité mentionné au I de l'article 9 sont mis en conformité avec celui-ci dans un délai de trois ans à compter de cette date. Les applications créées dans les six mois suivant la date de publication du référentiel sont mises en conformité avec celui-ci au plus tard douze mois après cette date* ».

Compte tenu de la date de parution de l'arrêté approuvant le RGS (18 mai 2010), la date limite fixée par l'ordonnance est le 19 mai 2013.

Pour les systèmes d'information relatifs aux marchés publics, cela signifie que la mise en conformité avec le RGS devait intervenir au plus tard le 19 mai 2013, et que depuis cette date, seuls les produits ou services conformes au RGS (ou à des conditions de sécurité équivalentes) peuvent être utilisés.

Les règles fixées sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage.

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité prévu par ce référentiel peut être attestée par une qualification.

L'ordonnance du 8 décembre 2005 prévoit que l'autorité administrative détermine pour chaque système d'information, après étude des risques, le niveau de sécurité requis parmi les niveaux prévus par le RGS (niveau *, ** ou ***). Les échanges intervenant via le système d'information doivent par la suite respecter les règles correspondantes. Pour les marchés publics, si le profil d'acheteur requiert un niveau de sécurité ** du RGS, tous les produits utilisés sur le profil d'acheteur, dont le certificat de signature électronique, devront correspondre au moins aux préconisations du niveau ** du RGS. Cela signifie que la plateforme devra reconnaître et accepter les produits de niveau ** et ***, mais pas ceux de niveau *.

II / Les certificats

Les documents qui doivent être signés par l'opérateur économique le sont au moyen d'un certificat de signature électronique. Pour les marchés publics, les principaux documents sont l'acte de candidature et l'acte d'engagement. Ces documents sont les seuls devant être signés par application du code des marchés publics.

[1] Ordonnance relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Le certificat électronique est une pièce d'identité électronique. Il contient l'identité du titulaire (une personne physique) et l'identité de la personne morale pour laquelle le certificat est délivré. Celui-ci est stocké sur une clé USB à crypto processeur, une carte à puce, ou sur le PC de l'utilisateur, selon le besoin de l'utilisateur (authentification ou / et signature).
Le RGS autorise la signature des documents électroniques en utilisant une clé privée associée à un certificat mono usage, dédié à la signature, ou à un certificat double usage combinant à la fois les fonctions d'authentification **et** de signature (mais il n'y a pas de certificats « double usage » de niveau 3 étoiles)

Les signataires utilisent le certificat de leur choix parmi l'une des trois catégories définies par l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics. Toutes les catégories de certificats conformes au RGS **ou à des conditions de sécurité équivalentes** sont utilisables (dès lors, bien sûr, que le certificat est utilisable pour les marchés publics : se renseigner auprès des prestataires sur les conditions de commercialisation[2])

Prestataires qualifiés et produits qualifiés

Des certificats de signature qualifiés RGS sont commercialisés par des *prestataires de services de confiance qualifiés*.
La liste des organismes habilités par l'ANSSI[3] à qualifier des *prestataires de service de confiance* est disponible à l'adresse suivante :
http://www.ssi.gouv.fr/fr/certification-qualification/qualification-d-un-prestataire-de-service-de-confiance/organismes-de-qualification-habilites.html

La société LSTI (La Sécurité des Technologies de l'Information), organisme accrédité par le COFRAC, est, au 15 avril 2013, la seule entité habilitée à qualifier des *prestataires de service de confiance qualifiés*.

Une liste des *prestataires qualifiés* au sens du RGS[4] figure sur le site de LSTI (auquel on accède également via celui de l'ANSSI : http://www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/):
http://www.lsti-certification.fr/

Il n'existe pas de liste officielle (ni même officieuse) des produits RGS commercialisés et utilisables pour les marchés publics.

Toutefois, en page d'accueil du site de LSTI, l'onglet « Prestataires qualifiés RGS » permet d'accéder à un tableau (format pdf) dénommé « Liste des prestataires de certification électronique qualifiés »
Ce tableau fournit les noms des prestataires et donne la liste, pour chacun d'eux, des produits ou services qu'il a développé et parmi lesquels, pour certains prestataires, figurent des certificats qui permettent la signature des candidatures et des offres[5].

Les sites Internet des prestataires ne renseignent pas toujours clairement sur les certificats de signature proposés.
Il est donc pratiquement toujours nécessaire (et prudent) de les contacter afin de connaître leurs produits, leurs conditions d'utilisation, et leurs coûts.

Certains de ces prestataires (ou Autorités de certification) commercialisent[6] des certificats permettant à des entreprises de répondre aux marchés publics (information à la date du 15 avril 2013, sous réserve de vérification) : l'Assemblée permanente des Chambres de Métiers, Certeurope, Certinomis, Chambersign

[2] Les certificats électroniques conçus par les prestataires ne sont pas tous des certificats de signature.
[3] Agence nationale de la sécurité des systèmes d'information
[4] Les prestataires peuvent également demandés à être qualifiés au sens des normes européennes ETSI (European Telecommunications Standards Institute) : TS 102 042 (qui équivaut, selon le niveau de confiance, au RGS 1 étoile ou 2 étoiles) et TS 101 456.
[5] La qualification de ces produits ou services relève de l'ANSSI.
[6] A la date du 15 avril 2013.

France (association créée par les Chambres de commerce et d'industrie), Click & Trust, Dhimyotis, Keynectis (l'onglet « certificats », en haut et à gauche de la page d'accueil, conduit au site Internet de SSL Europa, son distributeur), NATIXIS (mais uniquement auprès des entreprises ayant un compte ouvert chez NATIXIS), SG Trust Services (Société Générale)[7].

Certains produits font par ailleurs l'objet d'un référencement, lequel atteste que le certificat est interopérable[8]. On accède aux produits référencés par le lien suivant[9] :
http://references.modernisation.gouv.fr/liste-des-offres-r%C3%A9f%C3%A9renc%C3%A9es

Les listes de confiance

L'arrêté du 15 juin 2012 prévoit que le certificat de signature utilisé puisse appartenir à l'une des catégories de certificats délivrées par une autorité de certification figurant sur la liste de confiance d'un Etat-membre, telle qu'établie, transmise et mise à la disposition du public par voie électronique par la Commission européenne.

La « liste de listes de confiance » ainsi tenue par la Commission européenne (European Commission: List of Trusted List information as notified by Member States) permet d'accéder aux listes de confiance des Etats-membres.
Cette liste est provisoirement accessible sous format XML et sous format PDF aux adresses respectives suivantes :
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

La liste de confiance française (Trust-service Status List – TSL) est également disponible au format « machine » XML sur le site :
http://references.modernisation.gouv.fr/fr

Les informations figurant sur une liste de confiance permettent la vérification facilitée de la signature électronique ; mais ces listes ne citent généralement pas les produits ou services, seulement les entités bénéficiant de la confiance. Elles ne peuvent donc suffire à opérer le contrôle de la conformité ou de l'équivalence au RGS. En pratique, ces listent comportent des informations principalement destinées à des machines, les rendant inutilisables pour des personnes.

Le profil d'acheteur permet généralement d'assister le pouvoir adjudicateur dans la vérification de la signature électronique, la plateforme pouvant récupérer les éléments des listes de confiance disponibles en mode de lecture « machine » pour un examen automatisé du certificat de signature.

Il est donc possible, via la liste de confiance européenne, d'accéder aux TSL des Etats membres (notamment la liste de confiance française), c'est-à-dire aux entités habilitées à délivrer des certificats dont les autorités de certification des différents Etats considèrent qu'ils répondent aux exigences de sécurité fixées par ceux-ci[10].

Il est aussi possible d'accéder à ces listes de confiance par l'outil EU Trust Service status List (TSL) Analysis Tool disponible à l'adresse suivante :
http://eutsl.3xasecurity.com/tools/

---

[7] CRYPTOLOG International devrait commercialiser un produit d'ici septembre 2013, son dossier étant en cours de traitement par LSTI.

[8] Les certificats une étoile et les certificats « double usage » (authentification **et** signature) ne sont pas référençables ; seuls sont référençables les certificats de signature (mono usage) deux et trois étoiles, et les certificats d'authentification (mono usage) deux et trois étoiles.

[9] Il y a davantage de produits référencés que ceux qui figurent sur cette liste, mais ils sont utilisés en interne par le prestataire et ne sont donc pas commercialisés.

[10] De même que tous les prestataires qualifiés par LSTI ne conçoivent pas ou ne commercialisent pas des certificats permettant de soumissionner à un marché public, les produits ou services portés sur ces TSL ne sont pas tous conçus pour signer une candidature ou une offre.

Lorsque le certificat de signature émane d'une entité figurant sur la liste de confiance française ou d'une liste de confiance d'un autre Etat-membre, c'est-à-dire qu'il peut être relié à un prestataire ou un produit de sécurité référencé par la France ou, pour les autres Etats-membres, par la Commission européenne, la conformité du produit au RGS est présumée, et les seules vérifications à opérer sont celles du niveau de sécurité (*, ** ou *** ou leurs niveaux équivalents) et de la validité de la signature.

La responsabilité de l'acheteur

La vérification des certificats de signature électronique et de la validité de la signature elle-même font partie des fonctionnalités classiques d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner.

Toutefois, il faut insister sur le fait que, quel que soit le niveau d'automatisation des contrôles opérés, et quel que soit le résultat obtenu, l'acheteur a le pouvoir d'accepter ou de refuser une candidature ou une offre. Il en supporte bien sûr les conséquences, notamment en cas de contentieux ; si, en fonction des clauses de son contrat, la responsabilité du gestionnaire du profil d'acheteur peut être recherchée, elle n'exonère pas l'acheteur de sa responsabilité, la décision lui appartenant seul.

Logiquement, les certificats PRIS v1 ont vocation à disparaître, sauf à démontrer qu'ils garantiraient un niveau de sécurité équivalent aux prescriptions obligatoires du RGS.

Malgré l'échéance du 19 mai 2013, il est possible que certains profils d'acheteur refusent des certificats qualifiés RGS, ou au contraire continuent à accepter des certificats PRIS v1.
Si une certaine souplesse est acceptable dans les premières semaines de la date fatidique du 19 mai 2013, cette situation ne peut être que transitoire.

En tout état de cause, comme énoncé plus haut, l'acheteur devra systématiquement accepter tous les certificats qualifiés RGS, sous réserve que ceux-ci correspondent au niveau de sécurité (*, ** ou ***) rendu obligatoire par l'acheteur, principe qui vaut également pour tous les certificats équivalents au RGS.

Dans ce contexte, il ne faut pas non plus oublier que, comme pour les marchés non dématérialisés, la vérification de la capacité du signataire à engager l'entreprise reste à effectuer par l'acheteur (documents relatifs aux pouvoirs des personnes habilitées à engager les candidats).

La sécurité informatique trop souvent l’affaire de la seule DSI ?

Sécurité : Selon une étude PAC/Netasq, la sécurité est principalement l’affaire de l’informatique. Faute d’impliquer d’autres acteurs de l’entreprise, le facteur humain et ses vulnérabilités seraient insuffisamment pris en compte. Une vieille blessure soignée au pansement.

Par Christophe Auffray | Jeudi 21 Février 2013

D’après une étude du cabinet Pierre Audoin Consultants et de la société de sécurité Netasq, la sécurité informatique souffre d’une faiblesse majeure : elle reste cantonnée au service informatique, et omet trop souvent d’impliquer les autres acteurs de l'entreprise.

Ainsi dans 40% des cas, la sécurité informatique, au sens large (sécurisation des données clients, protection des employés et des actifs de l'entreprise), est prise en charge par le service IT. Seule une entreprise sur quatre a nommé un RSSI, une fonction il est vrai souvent limitée, pour des questions de coûts et de besoins, aux grandes entreprises.

La direction générale très impliquée dans la PSI

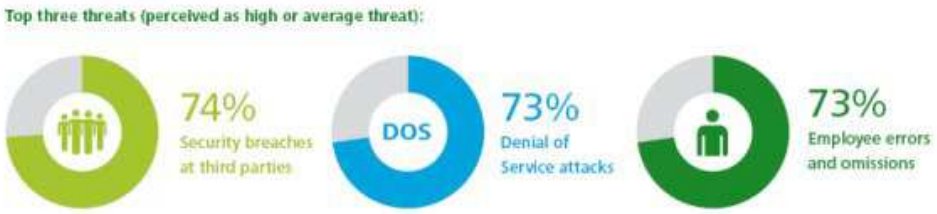
L’observation faite par le Clusif dans son rapport 2012 sur les menaces est toutefois plus nuancée avec une direction générale impliquée dans l’élaboration de la politique de sécurité dans 71% des entreprises (+16 points par rapport à 2010). Quand dans le même temps l’implication de la DSI et du RSSI recule.

Mais pourquoi l'implication d'autres fonctions de l'entreprise, en dehors de l'IT, est-elle nécessaire à la sécurité ? Notamment « pour s'ajuster efficacement aux nouvelles réglementations en constante croissance » répondent PAC et Netasq.

Ce n'est toutefois pas l'unique raison avancée. Une telle organisation centrée sur la DSI ne permettrait pas de prendre pleinement en considération le social engineering. Or, explique PAC, « la plupart des attaques récentes sont issues d'une défaillance humaine par l'utilisation des réseaux sociaux, l'usage inapproprié d'Internet ou encore par téléphone. »

Sensibilisation : tout le monde en parle, personne n'en fait ?

En clair, le facteur humain constitue une faiblesse, « une porte d'entrée » qu'une politique de sécurité ne peut omettre, au risque de se limiter à la mise en place de solutions techniques. Or selon l'enquête de Deloitte sur la sécurité informatique, les erreurs et omissions des salariés constituent une des trois principales menaces.

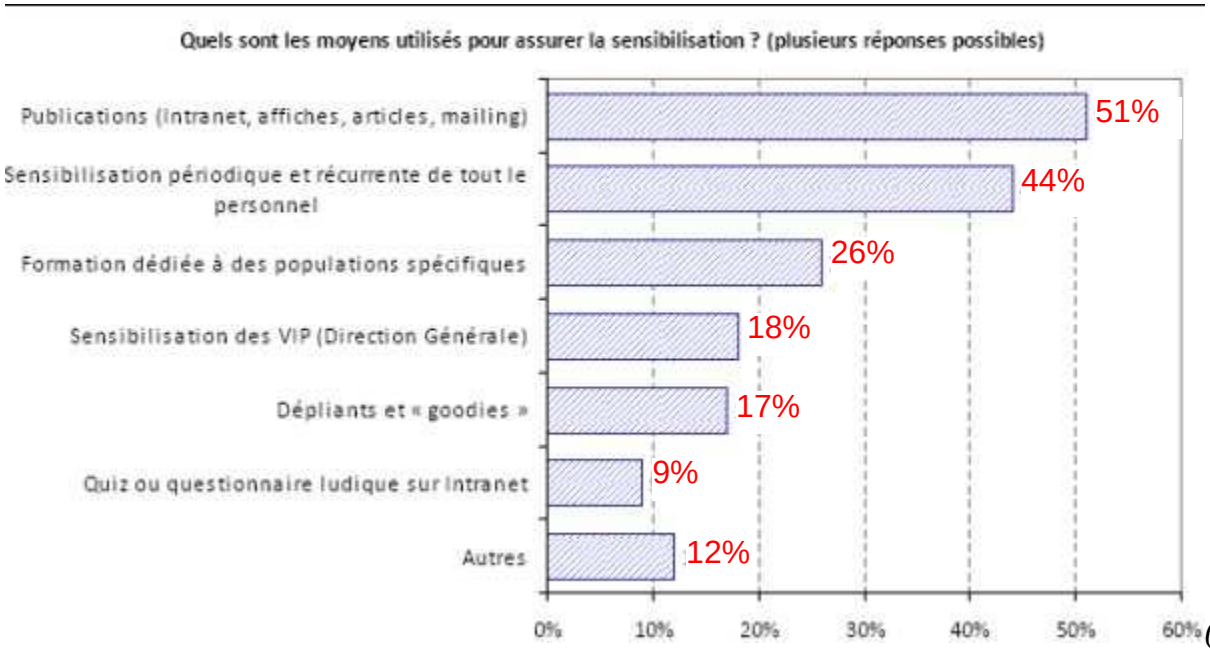


(Deloitte)

« Pour envisager une solution de sécurité informatique efficace, il faut au préalable réaliser des actions de sensibilisation sur l'ensemble des acteurs de l'entreprise sur le risque de ces attaques et de leur fournir les bonnes pratiques à avoir » préconisent donc PAC et Netasq.

Selon Deloitte, le manque de sensibilisation des salariés constituent en effet une source de vulnérabilités, notamment en raison de l'émergence de certaines pratiques comme par exemple le BYOD.

Mais compte tenu de l'ouverture des SI, la sensibilisation ne doit pas porter uniquement sur les employés, mais également sur les partenaires de l'entreprise. Néanmoins, si les spécialistes de la sécurité rappellent régulièrement la nécessité de mener des actions de sensibilisation, les entreprises restent encore trop souvent timides dans ce domaine.



(Clusif)

Dans son rapport 2012, le Clusif constate ainsi que « les programmes de sensibilisation à la sécurité de l'information sont toujours peu répandus ». Et que par ailleurs, la mesure de l'efficacité de ces programmes est tout aussi peu répandue.

Sensibilisation qui est encore plus le parent pauvre de la sécurité lorsqu'il s'agit des collectivités. « La sensibilisation des utilisateurs ne fait pas recette. La démarche semble s'essouffler puisque seules 17% des collectivités ont lancé des actions dans ce domaine et 12% en préparent. Soit à peu de chose près, la même proportion qu'il y a quatre ans » observe le Clusif.

Avez-vous oublié les fondamentaux ?

20 octobre 2011

Combien de personnes disposent du mot de passe administrateur permettant d'accéder au système central de gestion des droits ?
Il convient de réduire le nombre de titulaires de comptes disposant de privilèges élevés aux seules personnes pour lesquelles ces privilèges sont nécessaires à l'accomplissement de leur mission. Des listes doivent être tenues à jour pour tous les comptes de ce type, dont évidemment les comptes permettant d'accéder au système central de gestion des droits, qui constituent des cibles de choix pour les attaquants.

Quel mot de passe est utilisé pour installer une imprimante ? Le mot de passe permettant le contrôle total de votre système d'information, ou un autre ?
Le partage de mot de passe entre comptes doit être banni.

Chaque administrateur dispose-t-il d'un mot de passe différent ?
Afin de limiter les risques de compromission du mot de passe et de favoriser la traçabilité des actions, chaque individu doit utiliser un mot de passe personnel.

Lorsqu'un administrateur travaille à autre chose qu'à des tâches d'administration, quel type de compte utilise-t-il ?
Les comptes avec des droits d'administrateur doivent être strictement réservés à l'exécution de tâche d'administration. Des procédures doivent avoir été définies et une charte de l'administrateur établie afin de préciser ces conditions. Les administrateurs doivent utiliser un compte non privilégié lorsqu'ils effectuent des actions plus exposées, comme lire leurs courriels ou naviguer sur le web.

Quand, pour la dernière fois, quelqu'un a-t-il vérifié qui disposait des droits d'accès à la messagerie de votre PDG ou DG ?
Les accès à des ressources sensibles, comme la messagerie de dirigeants, doivent faire l'objet d'une surveillance régulière.

Qui a vérifié si, cette nuit, un fichier zip de 2 Go n'avait pas été extrait de votre système d'information ?

Quelqu'un regarde-t-il de temps en temps si les flux sortant de votre SI, la nuit par exemple, sont légitimes ? Si les adresses de destination sont normales ?

La dernière fois que vous êtes venus travailler un dimanche, quelqu'un est-il venu vous demander le lundi s'il était normal que quelqu'un se soit connecté sur votre compte dimanche ?
L'analyse des journaux d'événements permet de repérer les activités inhabituelles et de détecter d'éventuels signes d'intrusion. Les journaux d'événements doivent être activés, configurés et centralisés pour permettre cette analyse. De plus, le système utilisé doit permettre de générer des alertes simples et l'organisation doit prévoir le personnel et les procédures permettant de traiter ces alertes.

Votre propre poste de travail est-il à jour de ses correctifs de sécurité (pour l'ensemble des logiciels installés) ?
Il convient de mener un inventaire logiciel pour tous les postes de travail et d'utiliser un système centralisé de gestion des mises à jour pour corriger les vulnérabilités des logiciels inventoriés. Il ne suffit pas de mettre à jour uniquement le système d'exploitation, mais bien l'ensemble de logiciels déployés sur son parc.

Votre SI comporte-t-il encore des applications tournant sur Windows XP pack 2, voire 2000, voire même NT4 (on en voit plus souvent qu'on ne le penserait) ? Dans ce cas, quelles mesures de précaution ont été prises ?
Lorsqu'il n'est pas possible de migrer ces applications vers des systèmes maintenus par l'éditeur, il convient d'isoler de manière particulièrement restrictive et de porter une attention particulière à leurs journaux d'événements.

Quelqu'un a-t-il la cartographie de votre réseau - vraiment, pas juste une idée plus ou moins précise dans sa tête, mais un vrai schéma ?

(40) *ANSSI : Avez-vous oublié les fondamentaux ?*

Le maintien d'une cartographie à jour est indispensable pour pouvoir identifier les vulnérabilités et les corriger. Elle permet également de pouvoir réagir rapidement en cas de détection d'intrusion en limitant les risques de créer des dysfonctionnements par méconnaissance de son système d'information.

Combien d'accès internet avez-vous ? Où sont-ils ? Sont-ils tous administrés ? Surveillés ?
De trop nombreuses organisations laissent se multiplier les accès internet « sauvages », comme des lignes ADSL. Le résultat est une perte de capacité de surveillance des flux entrants et sortants et de blocage des flux illégitimes. Les accès sauvages échappent en effet aux systèmes de filtrage et de détection d'intrusion. Lorsqu'ils les identifient, des attaquants peuvent privilégier ces accès pour exfiltrer des données. Tout accès internet doit donc être recensé dans la cartographie et des règles de filtrage et de surveillance adaptées doivent y être associées. Le nombre d'accès doit être le moins élevé possible.

Combien de temps se passe-t-il entre le moment où quelqu'un quitte votre organisation et le moment où son compte est supprimé ?
Tout compte devenu inutile doit être immédiatement supprimé. Dans le cas contraire, un attaquant peut l'utiliser discrètement - qu'il s'agisse de l'ancien titulaire du compte ou d'un attaquant externe tirant profit de la situation. Une procédure adaptée doit donc être mise en place pour que le service informatique soit informé en cas de départ d'un employé et puisse supprimer ses droits d'accès. Lorsqu'une personne dispose d'un compte temporaire dans l'organisme (exemple : stagiaire, prestataire), une date d'expiration devrait être configurée dès la création du compte.

Combien avez-vous de comptes non individuels, de comptes de service ? À quoi servent-ils ?
Trop souvent les comptes partagés entre plusieurs individus ou de services possèdent des mots de passe faibles (type mot de passe = nom de compte) et qui n'expirent jamais. Or ces comptes permettent généralement d'accéder à de multiples ressources et, pour les comptes de services, disposent souvent de privilèges élevés. Pour ces raisons, ils sont l'une des premières cibles des attaquants. Il convient donc de tenir une liste de ces comptes et d'en mener une revue périodique pour en restreindre le nombre.

L'exécution automatique des supports usb est-elle désactivée ?
Les logiciels malveillants se diffusent très facilement par l'intermédiaire des supports USB lorsque l'exécution automatique de ces derniers est activée. Pour faciliter la gestion de cette fonctionnalité, vous pouvez utiliser des mécanismes de stratégie de groupe (GPO sous Windows) afin de désactiver les fonctions d'autorun et d'autoplay.

Les utilisateurs peuvent-ils installer des applications ?
Les utilisateurs ne doivent pas disposer de privilèges d'administrateurs. Par ailleurs, les stratégies de restrictions d'exécution logicielle (SRP et AppLocker sous Windows) restreignent l'exécution de logiciels malveillants et empêchent l'utilisateur de lancer un programme depuis un média amovible ou depuis son profil utilisateur. Il faut être vigilant aux environnements tels que Java, Adobe Air ou Perl, qui permettent d'exécuter des logiciels sans être contraints par les stratégies de restriction d'exécution logicielle.

Quel plan avez-vous en cas d'intrusion majeure dans votre système ?
Une intrusion d'ampleur dans un système d'information est une crise. Chaque heure qui passe peut notamment signifier la fuite d'informations stratégiques, avec dans certains cas, leur publication à des fins de déstabilisation. Des risques de suspension de l'activité de l'organisation sont aussi à prévoir. Un plan de réponse spécifique doit donc exister. Le plan de réponse doit prévoir les mesures organisationnelles et techniques permettant de délimiter au plus vite l'ampleur de la compromission et de la circonscrire. Par exemple, les documents nécessaires à la gestion de la crise, comme la cartographie du système, la liste des personnels en mesure d'intervenir sur les systèmes, les coordonnées des administrations susceptibles de porter assistance, doivent être tenus à jour et connus des personnels qui devront piloter la gestion de ce type de crise.

Que se passe-t-il quand vous découvrez un poste de travail compromis par un virus ? Le changez-vous simplement ou vérifiez-vous si par hasard l'attaquant n'aurait pas rebondi ailleurs dans votre système ?
La recherche d'éventuelles autres traces d'intrusion sur votre système est indispensable après la découverte d'une compromission. Généralement, les attaquants ne se contentent pas en effet de la compromission d'un ordinateur : ils s'ouvrent de multiples portes d'entrées dans le système afin de pouvoir revenir si d'aventure leur porte principale était refermée.

3. POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

- Effectuer une veille sur le site de l'ANSSI pour bénéficier des nouveaux guides de bonnes pratiques et de recommandations.
- La sécurité des systèmes d'information concerne tous les personnels dans leurs pratiques quotidiennes.
- Les services en charge de la sécurité des SI fonctionneront plus efficacement en réseau de façon à permettre les retours d'expérience et les échanges de bonnes pratiques entre les établissements.
- Des référentiels en matière de protection des SI existent déjà (ANSSI, RGS, norme ISO 27000...). Il est important de les appliquer.
- Etablir une démarche qualité et hygiène informatique (voir les règles et bonnes pratiques du guide). Diffuser les bonnes pratiques dans les entités.
- Contrôler et réglementer l'utilisation du « cloud computing » et les accès virtuels/à distance aux centres de calculs/ordinateurs.
- Crypter les données si besoin : clés USB, emails, ordinateurs ...
- Identifier les données à protéger (résultats de recherche non publiés, contrats...).
- Protéger les échanges de données sensibles : utiliser des outils de chiffrement et de signature et vérifier leur robustesse auprès des FSSI (fonctionnaires de sécurité des systèmes d'information des ministères).
- Établir une politique réaliste des accès à distance.
- Être vigilant vis-à-vis des certificats SSL : de faux certificats circulent (Google en a été victime en août 2011).
- Diffuser les pratiques dans toutes les entités des établissements.
- Identifier clairement la chaîne de décision dans l'établissement.
- Établir une chaîne de remontée des informations sur les incidents.
- Saisir le FSSI du ministère de tutelle en cas d'incident grave ou de questionnement.