RGPD

-

Notre engagement en 10 points

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. Un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment.

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.

Sécuriser les postes de travail

Les postes des collaborateurs 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.

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 » du collaborateur 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.

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.

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 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.

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.

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.

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.

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.

Angers, le 15 Octobre 2018

Julien Chardron

Romain Letué