Chapitre 1-3
Le référentiel sécurité

1. Introduction

L'élaboration d'un référentiel sécurité constitue un élément clé de la gestion en amont du risque cyber. Le référentiel sécurité correspond au corpus de politiques, chartes et procédures qui documentent les mesures de sécurité organisationnelles et techniques mises en place au sein de l'organisme.

Le référentiel sécurité comporte également des bonnes pratiques en matière de sécurité des systèmes d'information.

Dans ce chapitre, nous aborderons l'élaboration, la consolidation et la mise à jour de ce référentiel sous l'angle de la documentation des mesures organisationnelles, puis sous l'angle de l'encadrement juridique des relations contractuelles avec les sous-traitants et les partenaires.

2. La documentation des mesures organisationnelles et techniques

La documentation des mesures organisationnelles et techniques suppose la rédaction de différents livrables, tels que des plans, des chartes et des accords. Nous examinerons des stratégies de déploiement de chartes et de politiques internes, des plans de continuité et de reprise d'activité, ainsi que la maîtrise des normes techniques. Nous aborderons également le déploiement des audits internes et externes, les tests de résilience opérationnelle numérique et les autres mesures de prévention du risque cyber.

2.1 Décryptage des stratégies de sécurité cyber

La stratégie de sécurité cyber doit conduire à mettre en place différents documents tels que la charte administrateur, la politique de gestion des habilitations ou encore la politique de gestion des incidents.

2.1.1 Les mesures de protection de la charte « informatique »

La **charte « Utilisateurs des SI »** souvent dénommée **charte « informatique »** établit les conditions d'utilisation des systèmes d'information et de communication à disposition des salariés et vient préciser les pratiques possibles ou proscrites ou encore les sanctions en cas de non-respect de celle-ci. Les chartes informatiques et autres guides viennent donc formaliser les « instructions » de l'employeur sur l'utilisation de l'informatique. Il s'agit, du reste, d'une annexe au règlement intérieur de l'organisation soumise au même régime juridique.

Ces chartes ont pour objectifs d'informer le personnel et de formaliser par écrit les bonnes pratiques attendues et les comportements prohibés. Sous plusieurs aspects, ces documents remplissent un objectif de sensibilisation sur les sujets ayant trait à la sécurité informatique de l'organisme, et permettent de satisfaire aux obligations légales en la matière.

La charte vient encadrer les mesures d'investigations IT. Ces mesures d'investigations réalisées par les administrateurs sont la source d'un contentieux important et d'une jurisprudence abondante en constante évolution. Il est dès lors primordial de prévoir un encadrement adapté aux mesures d'investigation informatiques, tant du côté « utilisateur » que du côté « administrateur ».

La charte « Utilisateurs des SI » vient également encadrer l'utilisation de la boîte mail et d'Internet. En effet, le droit à la vie privée des salariés existe également sur le lieu de travail, y compris lors de l'utilisation de la messagerie professionnelle, d'Internet et du stockage de documents sur les serveurs de l'entreprise dès lors que ces usages et fichiers sont clairement identifiés comme personnels. Un cadre strict doit en effet être défini par l'employeur afin d'éviter tout abus, tout en s'attachant au respect des principes de transparence et de proportionnalité régulièrement débattus au sein d'une jurisprudence riche et subtile.

Cas d'école en matière de « cybercriminalité interne », les actions de téléchargement de données par le personnel doivent suivre une procédure pragmatique, conciliant les impératifs pratiques liés à la vie de la structure avec les besoins de contrôle et de sécurité (supports, environnements, autorisations préalables…). La charte encadre donc ces actions.

Il est également indispensable d'encadrer les usages du matériel et des outils informatiques utilisés par le personnel.

Ainsi les chartes présentent des enjeux juridiques essentiels et stratégiques qui se cristallisent autour de trois points cruciaux :

– Respect de la vie privée : quelle tolérance accorder au salarié/agent sur l'utilisation de la messagerie électronique, d'Internet, du téléphone professionnel ? Quel comportement attendre du salarié/agent ? Comment m'assurer que les mesures de contrôle mises en place sur les systèmes informatiques restent conformes au cadre légal ?
– Preuve : comment rendre admissibles et opposables les éléments de preuve collectés lors d'investigations informatiques ? Quels garde-fous mettre en place ? Quelles procédures adopter selon les différentes situations de contrôle (routine, crise cyber…) ?

– Fraude : comment définir le comportement fautif ? Comment m'assurer que ma charte informatique est opposable au salarié/agent ? Comment m'assurer que la fraude sera retenue par le juge ? Quelles précautions mettre en place pour m'assurer de l'opposabilité réelle de la charte informatique ?

2.1.2 La charte « Administrateurs des SI »

Certains employés et collaborateurs, du fait de leurs habilitations particulières et de leur rôle dans « l'administration » au quotidien des différents systèmes d'information déployés (internet/intranet, smartphones, téléphone...), ont vocation à voir leurs actions encadrées par des dispositions spécifiques, dispositions formalisées au sein d'une **charte « Administrateurs des SI »**.

Cette charte est en effet l'un des piliers essentiels du référentiel sécurité d'une entité qu'elle soit publique ou privée. Ce document participe directement à répondre à l'impératif de documentation des mesures organisationnelles et techniques visées par le RGPD.

Plus précisément, les personnes visées par la charte « administrateurs des SI » sont les éléments clés du système d'information (SI) mais également les contributeurs majeurs de la sécurité dudit SI. Les administrateurs se distinguent ainsi des autres utilisateurs par les droits étendus qui leur sont accordés sur le SI et constituent à ce titre une ressource critique pour les entreprises. La charte « administrateurs des SI » a donc vocation à encadrer l'exercice de ces droits étendus.

Conformément aux dispositions de l'article 24 du RGPD, l'ANSSI rappelle que la sécurité des systèmes d'information nécessite la mise en œuvre de mesures de sécurité techniques et organisationnelles appropriées pour garantir la sécurité des données. C'est à ce titre que la charte « administrateurs des SI » constitue une documentation indispensable pour tout responsable de traitement.

Cet outil a pour finalité d'établir un équilibre entre les pouvoirs spécifiques accordés aux administrateurs et le respect d'obligations indispensables à la sécurité du SI.

Les objectifs principaux poursuivis

D'une manière générale, la charte vise à assurer :

– la protection des droits des personnes dont les données sont traitées dans les systèmes d'information,
– la confidentialité des données,
– la sécurité du système d'information.

À cet égard, elle a vocation à compléter le « Référentiel Sécurité » et plus particulièrement la charte d'utilisation des systèmes d'information.

Ce que doit contenir une charte « Administrateurs des SI »

La charte doit tout à la fois prévoir les règles de sécurité que l'administrateur devra respecter et établir les objectifs et les limites de l'intervention de l'administrateur sur le SI.

À ce titre, elle devra informer chaque administrateur désigné au sein d'une entité :

– *De ses obligations en termes de sécurité et de bon fonctionnement des SI pour lesquels il esthabilité à intervenir*

  L'administrateur a notamment pour rôle d'assurer le bon fonctionnement général des systèmes d'information (performance, disponibilité, interopérabilité...) et de veiller à la bonne utilisation des systèmes d'information (administration des habilitations et des profils, gestion de l'utilisation des messageries et des accès à internet, etc.)

– *Des moyens à sa disposition pour assurer sa fonction et des limites de son utilisation des outils*

  Pour garantir la sécurité du SI, les moyens mis à sa disposition et son périmètre d'action devront être précisément circonscrits (postes informatiques, serveurs, connexion, accès distants, applications, etc.)

– *De son obligation de confidentialité au regard des données traitées*

  La CNIL rappelle que les administrateurs sont contraints à une obligation de confidentialité renforcée. Cette obligation de confidentialité renforcée porte sur l'ensemble des informations et données dont l'administrateur pourrait avoir connaissance dans le cadre de ses fonctions à l'exclusion des seules données publiques.

– *Des modalités de gestion des mots de passe spécifiques à ses fonctions.*

  Le rôle principal de l'administrateur est de veiller à la sécurité des systèmes d'information et notamment de respecter la plus stricte confidentialité des mots de passe et notamment de son mot de passe administrateur.

2.1.3 La politique de gestion des habilitations

La politique de gestion des habilitations est une mesure organisationnelle interne faisant partie intégrante du référentiel sécurité des entreprises.

Elle a vocation à encadrer les accès aux SI :

– **Par les acteurs internes de l'entreprise** : salariés, contractuels, intérimaires, consultants ou stagiaires

– **Par les acteurs externes amenés à intervenir sur le SI** : prestataires informatiques, auditeurs, etc.

L'élaboration de cette documentation permet :

– en amont : de recenser les accès ouverts pour chaque catégorie d'acteurs et d'effectuer un état des lieux des éventuelles habilitations illégitimes,

– de définir des ensembles de ressources pour lesquels différents niveaux d'habilitation s'imposent,

– de définir des décideurs aux habilitations : DSI, directeurs, responsables de service, etc.,

– de définir des profils d'habilitation par service ou par type de poste et des habilitations unitaires lorsque cela est pertinent,

– d'informer les acteurs sur l'étendue de leurs droits afin de préserver la responsabilité de l'entreprise.

Cette documentation répond à plusieurs impératifs identifiés par la CNIL et mis à la charge des responsables de traitement. L'obligation de définir des niveaux d'habilitation est un corollaire du principe de minimisation résultant de l'article 5.1.c du RGPD lequel impose de limiter les activités de traitement aux données strictement nécessaires au regard des finalités poursuivies. La Commission en déduit que l'accès des utilisateurs (internes ou externes) doit être limité aux seules données strictement nécessaires à l'accomplissement de leurs missions.

À titre de précautions élémentaires, il est conseillé de définir des profils d'habilitation et de réaliser une revue annuelle des habilitations afin de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Pour documenter cette conformité, la CNIL conseille d'établir et de réexaminer régulièrement une politique de contrôle des habilitations devant inclure :

– les procédures à appliquer lors du départ, de l'arrivée ou du changement d'affectation d'un utilisateur du SI,
– les conséquences d'un accès illégitime aux données en cas de non-respect des mesures de sécurité,
– les mesures permettant de restreindre et de contrôler l'attribution des habilitations.

Les risques liés à la gestion des habilitations

Des défaillances dans la gestion des habilitations peuvent induire de véritables vulnérabilités pour le SI. Différentes hypothèses sont envisageables :

– méconnaissance du périmètre effectif des habilitations pouvant conduire à des attributions d'habilitation dépassant le périmètre souhaité,
– attribution d'une habilitation à la mauvaise personne ou sur la base d'une qualité fausse et non vérifiée,
– absence de mise à jour des habilitations entraînant un maintien d'habilitation injustifié (par exemple lors d'un changement de poste ou d'un départ),
– attribution à un même acteur d'habilitations incompatibles.

Ces vulnérabilités sont susceptibles d'induire des incidents de sécurité et des violations de données au sens de l'article 4.12 du RGPD et de contraindre le responsable de traitement à notifier l'autorité de contrôle, l'exposant ainsi à de lourdes sanctions.

Sans même qu'il soit nécessaire d'envisager l'hypothèse d'un acte malveillant, ces différents scénarii sont susceptibles de constituer une violation affectant l'intégrité ou la sécurité des données :

– consultation de données par une personne qui ne devrait pas y être autorisée,
– modification ou suppression de données par une personne qui ne devrait pas être autorisée à y accéder,
– déclenchement de processus de contrôle du SI par une personne qui ne devrait pas y être autorisée (arrêt de composants du système, installation de logiciels malveillants ou non).

Les prérequis à la gestion des habilitations

Pour que les habilitations puissent être définies et traduites en autorisations d'accès pour chaque utilisateur du SI, certaines fonctions doivent au préalable être mises en œuvre :

– l'enregistrement et l'identification des acteurs,
– l'authentification des acteurs,
– un inventaire des ressources (données, traitements informatiques outils…) qui doivent faire l'objet d'un contrôle d'accès,
– le modèle retenu pour l'organisation et l'attribution des habilitations doit être déterminé (profils d'habilitation, habilitations unitaires).

Définir la politique d'authentification

L'habilitation des utilisateurs des systèmes d'information repose sur une politique d'authentification établie par l'entreprise. Cette authentification permet d'identifier l'utilisateur qui se connecte au SI et est un prérequis indispensable à la bonne gestion des habilitations.

Pour des raisons évidentes de traçabilité, toute personne doit être identifiée et authentifiée de manière sécurisée et certaine avant qu'elle ne puisse agir sur le SI (consultation, modification, téléchargement, suppression…).

Compte tenu des informations accessibles sur ses systèmes d'information, il relève de la responsabilité du responsable de traitement de mettre en place une authentification sécurisée et en cohérence avec le niveau des droits attribués à chaque utilisateur.

D'une manière générale la règle doit être la suivante : plus l'utilisateur aura un niveau étendu d'accès à des informations confidentielles, plus son niveau d'authentification devra être fort.

2.1.4 L'importance de la politique de mot de passe efficace

La création et la conservation d'un mot de passe obligent les utilisateurs à faire preuve d'une grande créativité : nombre minimum de caractères, interdiction d'utiliser des dates de naissance, obligation d'insérer des caractères spéciaux, interdiction d'utiliser des mots du dictionnaire…

Ces limitations revêtent une importance primordiale à l'heure où, comme le révèle une étude de Verizon, environ 80 % des violations de données résultent d'attaques par force brute, c'est-à-dire du test successif des combinaisons possibles d'un mot de passe ou de l'utilisation d'identifiants perdus ou volés.

Pour se prémunir d'une telle attaque, les organismes doivent mettre en place une politique de mot de passe. En effet, l'article 5-1-f) du RGPD met à la charge du responsable de traitement une obligation de sécurité des données traitées, sécurité qui passe notamment par une utilisation encadrée des mots de passe.

C'est dans l'optique d'aider les organismes à mettre en place la politique de mot de passe que la CNIL a publié le 17 octobre 2022 une version actualisée de sa recommandation sur le sujet.

La CNIL, dans sa nouvelle recommandation, souligne la nécessité de conditionner la sécurité à l'utilisation de procédures et politiques conformes à la réalité des opérations réalisées en rappelant que « *la taille et le contenu de la liste de mots de passe à refuser doivent être proportionnels aux risques et, le cas échéant, adaptés au contexte d'usage*. »