Sécurisez vos fichiers

obligations procédures nominatifs contrôles

Principauté de Monaco

Commission de Contrôle des Informations Nominatives

Vous êtes chef d'entreprise, profession libérale, artisan, commerçant, président d'une association, responsable d'un organisme public, etc :

- Votre système informatique stocke des données à caractère personnel ?
- Vous disposez d'un réseau d'entreprise qui permet l'accès à des informations nominatives ?
- Vous échangez des données avec vos partenaires ou clients ?
- Vous diffusez des informations nominatives sur Internet ?
- Vos collaborateurs utilisent des terminaux mobiles ?

> « VOUS DEVEZ ASSURER LA PROTECTION DE VOS DONNEES ! »

Sommaire

La Commission de Contrôle des Informations Nominatives est une Autorité Administrative Indépendante instituée par la loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives.

Elle a pour mission de veiller au respect des libertés et droits fondamentaux des personnes dans un domaine particulier : l'utilisation de leurs données personnelles.

Or dans le cadre de sa mission de contrôle, la Commission a constaté que certains responsables de traitement (cf. lexique) ne garantissaient pas suffisamment la sécurité des données nominatives qu'ils exploitaient.

> « LA LOI IMPOSE AUX RESPONSABLES DE TRAITEMENT DES OBLIGATIONS DE SÉCURITÉ ET DE CONFIDENTIALITÉ ! »

Les enjeux

Assurer la sécurité et la confidentialité des données, c'est protéger toute information dont la compromission pourrait porter atteinte aux droits des personnes protégés par le Titre III de la Constitution (respect de la vie privée et du secret des correspondances, liberté d'opinion, etc), mais également à la sécurité nationale, à des intérêts économiques ou technologiques, ou encore à l'image d'une société.

Ce guide a donc pour vocation de présenter les préconisations minimales d'ordres technique et organisationnel en vue d'assurer la sécurité d'un traitement d'informations nominatives et la confidentialité des données qu'il contient.

Par sécurité, il convient d'entendre la limitation des risques inhérents à l'exploitation d'un traitement automatisé ou non automatisé d'informations nominatives (cf. lexique).

CONSIDERATIONS PREALABLES : EVALUER LES RISQUES

La sécurité d'un système d'information repose sur trois principes fondamentaux :

- **Confidentialité :** seules les personnes habilitées doivent avoir accès aux informations ;
- **Intégrité :** les données ne doivent pas être altérées durant leur collecte, leur exploitation, leur transfert, etc ;
- **Disponibilité :** il convient de garantir l'accès aux ressources tant en termes de délai que de qualité.

A la lumière de ces principes, l'évaluation des risques de sécurité d'un système d'information est un préalable indispensable à l'adoption de tout mécanisme de protection par le responsable de traitement. A ce titre, il convient :

- de déterminer, dans le cadre d'un audit du système d'information, les besoins du responsable de traitement au regard des activités de la structure et des objectifs recherchés (étape 1) ;
- d'identifier les différents risques et le degré de menace qu'ils représentent (étape 2) afin de mettre en œuvre une politique de sécurité adaptée (étape 3).

> « PRINCIPE DE PROPORTIONNALITÉ DE LA POLITIQUE DE SÉCURITÉ »

La loi n° 1.165 impose l'adoption de mesures de sécurité permettant d'assurer *" un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger "*.

Autrement dit, inutile d'envisager des mesures extrêmement coûteuses et à la pointe de la technologie, si cela n'est pas nécessaire au regard de la sensibilité des données à protéger et des menaces pesant sur ces dernières !

ETAPE 1 : LA CONDUITE D'UN AUDIT

L'audit a pour objectif d'identifier les besoins de la structure au regard de ses activités. Cette démarche implique :

- de recenser les informations nominatives exploitées (nom, prénom, date de naissance, identifiant, adresse IP (cf. lexique), etc) et les traitements automatisés ou non automatisés dans lesquels elles figurent (fichiers clients, fichiers du personnel, messagerie, vidéosurveillance, systèmes biométriques de contrôle d'accès, etc) ;
- de s'assurer que ces informations sont véritablement nécessaires à la finalité pour laquelle elles sont collectées et traitées, et plus généralement, pour les activités de la structure ;
- de déterminer le niveau de sensibilité de ces données ;
- de lister les personnes qui ont accès aux traitements ;
- d'identifier les différents supports sur lesquels ces traitements sont exploités ou rendus accessibles (ordinateurs, téléphones portables, clés USB, CD, serveurs, tablettes, documents papier, etc).

Il est conseillé de réaliser cet audit en équipe, en la présence des administrateurs systèmes, des responsables hiérarchiques, et le cas échéant, des utilisateurs. Un audit devra également être conduit préalablement au déploiement de toute nouvelle solution technique, informatique ou organisationnelle aux fins d'apprécier les implications en matière de protection des données personnelles (nouvelles formalités à accomplir auprès de la CCIN, etc).

ETAPE 2 : L'ANALYSE DES RISQUES

Il s'agit de répertorier et de classifier les différentes menaces qui pèsent sur chaque support d'exploitation des données et d'estimer leur probabilité de survenance.

Les menaces sont de plusieurs types : perte ou vol de données, détérioration du parc informatique, détournement de l'usage d'informations, espionnage.

L'actualité regorge d'exemples à ce sujet : perte d'une clé USB, destruction d'un disque dur, vol de *smartphones* ou d'ordinateurs portables, intrusion dans un système informatique, etc.

La meilleure approche pour analyser l'impact d'une menace - autrement dit sa gravité - consiste à déterminer à quel point la vie privée des personnes pourrait être affectée par sa survenance.

Certains exemples sont particulièrement significatifs : piratage d'une base informatique contenant des pièces d'identité numérisées (usurpation d'identité), ou encore vol de données bancaires (fraude aux moyens de paiement).

L'appréciation des risques doit mettre en balance d'une part, la gravité des menaces identifiées, et d'autre part, leur probabilité de survenance. C'est sur cette base que pourra être décidée la mise en œuvre de mesures de sécurité proportionnées et adaptées.

ETAPE 3 : LA FORMALISATION D'UNE POLITIQUE DE SÉCURITÉ

Une fois les traitements recensés et les risques identifiés et classifiés, il convient de formaliser les règles de procédure interne.

Leur ensemble constitue la politique de sécurité de la structure, laquelle doit être conduite en toute transparence afin de garantir son efficacité.

Ainsi, toute procédure concernant le personnel doit être expressément portée à sa connaissance - par exemple par le biais d'une charte informatique (cf. *infra* p.8).

La politique de sécurité devra être régulièrement mise à jour. Pour ce faire, il est conseillé de procéder à des audits réguliers afin de s'assurer que les procédures sont correctement appliquées et cohérentes avec l'évolution du système d'information de la structure.

La sécurité informatique repose sur une bonne connaissance des règles par l'ensemble des intervenants et utilisateurs des traitements.

A ce titre, il est recommandé de prévoir la signature d'un engagement de confidentialité pour les prestataires, ou, pour les salariés, l'insertion de clauses spécifiques à la protection des données personnelles dans le contrat de travail.

01 Les mesures organisationnelles

Les procédures internes et la charte informatique

La charte informatique est un document écrit ayant vocation à encadrer les droits et obligations des utilisateurs d'équipements ou de ressources informatiques.

Elle permet également de participer à la sensibilisation des personnes à la protection des données personnelles, et plus généralement, au respect des droits d'autrui (respect de la vie privée et familiale et du secret des correspondances, droits de propriété intellectuelle, etc).

Une charte revêt généralement une valeur contractuelle, notamment lorsqu'elle est annexée au contrat de travail ou de prestation, ou acceptée par un utilisateur sur Internet (ex. charte de forum en ligne ou de tout autre site hébergeur de contenus).

A minima, la charte informatique doit aborder, si applicable, les problématiques suivantes :

1. les modalités d'usage des équipements mis à la disposition des collaborateurs par l'employeur (PC, téléphones, équipements nomades, etc), notamment en ce qui concerne leur utilisation à des fins privées ;
2. de même, les modalités d'exploitation des outils informatiques et ressources (Internet, Intranet (cf. lexique), messagerie, etc) ;
3. les diverses mesures mises en place pour contrôler les utilisations susvisées (outils d'administration système, dispositifs d'alerte, traçabilité du système d'information, etc) ;
4. les personnes habilitées à avoir accès aux traitements ainsi que les modalités et procédures d'accès ;
5. le rappel des règles de droit applicables en matière de protection des données personnelles et de respect des droits des personnes (modalités d'exercice des droits d'accès, de modification, de suppression voire d'opposition de la personne concernée) ;
6. le rappel des procédures de sécurité en matière d'accès (authentification) et d'échanges de données, ainsi que les remontées d'alertes aux services compétents en cas de soupçon de défaillance ;
7. les responsabilités et sanctions encourues en cas de violation des dispositions de la charte.

Lorsque sont développées des solutions de surveillance ou de traçabilité du système d'information, la charte constitue un excellent support d'information des personnes concernées, comme le requiert l'article 14 de la loi n° 1.165, modifiée.

A cet égard, les spécificités afférentes à l'exploitation de dispositifs de contrôle d'accès (biométriques ou non), de vidéosurveillance, de géolocalisation, ou encore de supervision de la messagerie ont été rappelées dans le cadre de diverses délibérations de la CCIN, disponibles sur son site Internet (**www.ccin.mc**).

En matière de supervision de la messagerie, notamment, la Commission demande la mise en place d'une procédure interne, garantissant le respect du secret des correspondances, tout en permettant à l'employeur d'exercer une supervision proportionnée et strictement nécessaire à la réalisation d'objectifs déterminés et justifiés.

D'une manière générale, il est recommandé de formaliser toutes les procédures internes, la transparence de telles procédures constituant une condition nécessaire à leur effectivité.

Par ailleurs, il pourrait être envisagé l'établissement d'une charte de sécurité spécifique aux administrateurs informatiques.

En effet, dans le cadre de leurs missions de travail, les administrateurs informatiques possèdent des droits d'accès privilégiés aux ressources du système d'information. De ce fait, ils sont susceptibles d'avoir connaissance de données personnelles, voire sensibles, dont ils ne sont pas les destinataires.

Il convient donc de définir strictement leurs missions, de préciser leurs droits d'accès et de rappeler en particulier qu'ils ne sauraient faire un usage abusif de tels droits.

Les habilitations et la gestion des accès aux données

Sécuriser un système d'information - et garantir la confidentialité des données qu'il contient - nécessite en tout premier lieu de contrôler qui a accès à ce système, et suivant quelles modalités.

Ce contrôle peut revêtir plusieurs aspects :

- le contrôle des accès logiques à travers un système d'authentification ;
- la gestion de l'étendue de ces accès par des procédures d'habilitation ;
- le contrôle des accès physiques aux locaux contenant les équipements essentiels (cf. *infra* p. 14).

Il est recommandé de rappeler tout ou partie des principes qui vont suivre dans le cadre de la charte informatique.

L'AUTHENTIFICATION DES UTILISATEURS

L'authentification est un processus permettant de s'assurer de l'identité d'un utilisateur.

Elle inclut deux actions. Généralement, il s'agit de la saisie de l'identifiant de l'utilisateur (*login*), puis d'un mot de passe (*password*) qui vient authentifier l'identité déclarée. Certains systèmes peuvent également prévoir, plutôt qu'un mot de passe, la lecture d'une carte à puce ou dans le cas de systèmes biométriques, la présentation de la paume de la main, de l'index, de l'iris, etc.

Une authentification est qualifiée de forte lorsqu'elle cumule au moins deux facteurs d'authentification (ex. mot de passe + carte à puce, token, clé USB, etc).

Dans certains cas, l'authentification peut être implicite, héritée d'une authentification précédente, voire reconnue automatiquement (ex. après analyse de l'adresse IP). D'une manière générale, ce type de mécanisme est déconseillé.

Le choix du mot de passe

Si l'identifiant peut dans certains cas être imposé, il doit néanmoins être différent du mot de passe, lequel doit respecter certaines règles impératives :

- **Il doit être INDIVIDUEL, SECRET et SPECIFIQUE**
  Vous devez être le seul à le connaître. Par principe, il est risqué de le communiquer à un tiers. Evitez aussi de le noter sur un pense-bête.

  En outre, un mot de passe ne doit servir que pour une action particulière. Ainsi, il est déconseillé d'utiliser le même mot de passe pour déverrouiller son ordinateur, accéder à des sites marchands, ouvrir des dossiers personnels, etc.

- **Il doit être COMPLEXE**
  Evitez les mots de passe simplistes que l'on peut deviner (dates d'anniversaire, prénoms des enfants ou de l'animal de compagnie, suite de chiffres).

  Ainsi, un mot de passe efficace doit comporter au moins 8 à 10 caractères incluant chiffres, lettres et caractères spéciaux.

  Vous pouvez par exemple avoir recours à une phrase mnémotechnique telle que " *Mon mot de passe est difficile à découvrir !* ", qui pourrait être traduit comme suit : " *Mm2pedàd!* ".

En tout état de cause, afin de rendre cette protection encore plus efficace, il est nécessaire de :

- renouveler son mot de passe régulièrement ;
- prévoir un verrouillage automatique du terminal après un certain laps de temps sans activité.

Remarque : Il existe des systèmes d'authentification forte basés sur le principe du mot de passe à usage unique (*One Time Password* ou OTP) et dont la durée de vie n'excède pas la minute. Cela permet d'éviter qu'un mot de passe soit volé et réutilisé. Ce type d'authentification est généralement utilisé pour des accès externes via VPN (cf. *infra* p. 22).

LES PROCEDURES D'HABILITATION OU LA GESTION DES DROITS D'ACCES

L'habilitation est fonction d'un profil préalablement défini, généralement lié à une position hiérarchique ou à une fonction au sein de la structure, et non à une personne physique déterminée.

Cela permet de faciliter la gestion des accès en cas de mouvement de personnel. Au contraire, lorsque les accès sont attribués par personne, il convient d'être extrêmement réactif et de supprimer tout accès en cas de départ d'un membre du personnel du service ou de la structure.

L'habilitation doit conférer à chaque utilisateur les droits qui sont strictement nécessaires à l'accomplissement de ses attributions. A ce titre, elle doit déterminer, notamment :

- les données et applications auxquelles celui-ci peut avoir accès, de manière dédiée ou partagée (réseau local ou partagé, dossiers de travail, imprimantes, etc) ;
- l'étendue des droits ainsi conférés : accès en simple consultation, en inscription, en suppression.

Lorsqu'il s'agit d'accès vers des traitements d'informations nominatives relevant des articles 11 et 11-1 de la loi n° 1.165, modifiée, l'article 17-1 de cette même loi impose au responsable de traitement d'établir et de tenir à jour la liste nominative de ces personnes. Cette liste doit pouvoir être fournie à la CCIN à tout moment sur simple réquisition.

En cas de multiples tentatives d'accès infructueuses, il peut être prévu un mécanisme de blocage temporaire du compte utilisateur, que seul l'administrateur système peut débloquer. L'existence de ce dispositif de sécurité doit, le cas échéant, être signalée dans la charte informatique.

Enfin, il convient de rappeler que le traitement automatisé afférent à la gestion des habilitations est soumis aux formalités prévues par la loi n° 1.165, modifiée.

Le recours à la prestation de service

Un responsable de traitement peut recourir aux services d'un prestataire, notamment à des fins d'administration du système lorsque celle-ci n'est pas effectuée en interne, ou encore, pour assurer la maintenance des équipements.

Dans ce cas, il doit assurer la sécurité et la confidentialité des données auxquelles le prestataire est susceptible d'avoir accès. Il convient donc de prévoir un engagement de confidentialité qui explicite, notamment, les points suivants :

1. les obligations de sécurité et de confidentialité du prestataire ;
2. le droit de propriété du responsable de traitement sur ses données et l'absence de toute licence ou cession de droits implicite sur ces dernières au prestataire ;
3. l'interdiction ou l'autorisation conditionnelle de sous-traiter la prestation ;
4. la possibilité de vérification par le responsable de traitement du respect des obligations susvisées et de l'effectivité des mesures prises à cet effet ;
5. les modalités de restitution du matériel et d'effacement de toute donnée personnelle dupliquée chez le prestataire au terme d'opérations de maintenance ou du contrat de prestation, sauf instructions contraires du responsable de traitement ;
6. les modalités de maintenance ou de télémaintenance.

La télémaintenance permet l'accès à distance aux équipements et données exploitées par le responsable de traitement. Elle présente donc un risque potentiel pour la sécurité des données. De par son caractère intrinsèquement intrusif, il est recommandé d'assurer la plus grande transparence dans son déroulement.

C'est pourquoi il est conseillé de s'assurer que le prestataire :

1. s'engage à obtenir l'accord préalable du responsable de traitement avant chaque opération de télémaintenance (planification) ;
2. permette à celui-ci d'identifier la provenance de chaque intervention distante ;
3. consigne, pour chaque opération de télémaintenance, les dates, la nature des opérations et les noms des intervenants, afin de pouvoir en justifier auprès du responsable de traitement.

Les mesures de sécurité physique

La sécurité des données repose sur celle des équipements qui servent de support à leur exploitation informatique, et donc sur celle des locaux où ces équipements sont situés.

Des mesures de sécurité physique sont donc nécessaires afin de protéger ces locaux contre tout dommage matériel, ainsi que contre l'intrusion de personnes non habilitées.

LA VIDEOSURVEILLANCE

Il est recommandé de placer sous vidéosurveillance les locaux sensibles, tels que ceux comprenant le système informatique. Toutefois, ce dispositif ne saurait être utilisé à des fins de surveillance du personnel. Ainsi, des caméras fixes orientées exclusivement vers les équipements à protéger doivent être privilégiées.

Le responsable de traitement est tenu de soumettre un tel traitement aux formalités légales prévues par la loi n° 1.165, modifiée. A cet égard, son exploitation doit répondre, selon le cas, aux termes de la délibération n° 2010-13 du 3 mai 2010 (vidéosurveillance sur le lieu de travail), ou de la délibération n° 2011-83 du 15 novembre 2011 (vidéosurveillance dans les immeubles d'habitation).

LE CONTROLE D'ACCES

Il peut être envisagé la mise en place de systèmes de contrôle d'accès par carte, digicode, etc. Ces systèmes impliquent l'exploitation de traitements soumis à formalités légales.

Ils permettent de réguler les accès au sein même de la structure, par une attribution justifiée des droits d'accès en fonction des missions du personnel (plages horaires, type de locaux) ou des prestataires et des visiteurs.

En cas de recours à des systèmes biométriques, trois délibérations de la Commission encadrent leur exploitation (délibérations n° 2011-31, n° 2011-32 et n° 2011-33 du 11 avril 2011 disponibles sur **www.ccin.mc**).

A cet égard, il convient de rappeler les principes généraux suivants :

- la biométrie sans trace doit être privilégiée (réseau veineux, contour de la main) ;
- la biométrie ne doit pas être envisagée comme une finalité de confort, mais être strictement justifiée par des motifs impérieux ;
- le recours aux dispositifs d'accès par lecture de l'empreinte digitale n'est possible que pour contrôler l'accès à certaines zones limitativement identifiées de la structure, à condition que l'empreinte soit stockée sur un support individuel détenu par la personne concernée, à l'exclusion de tout enregistrement centralisé dans une base.

LES MESURES PARTICULIERES CONCERNANT LE LOCAL INFORMATIQUE

Le système informatique doit être situé dans des locaux climatisés, dont l'accès est réservé au seul personnel habilité. Ces locaux doivent comprendre l'ensemble des équipements techniques sensibles tels que serveurs, routeurs, commutateurs, etc.

Le matériel informatique ne doit pas être mis à même le sol, mais être surélevé (ex. dans une baie informatique).

Une attention particulière devra être portée à la mise en place de panneaux d'interconnexion réseau (brassage de câbles, de connecteurs RJ45, etc).

02 Les mesures techniques

Les mesures de protection

LES PARE-FEU, ANTIVIRUS ET *PROXIES*

Il existe diverses mesures techniques ayant vocation à protéger un système (réseau, PC) en amont contre les intrusions de toute nature.

1. Les pare-feu (*firewall*)

Il s'agit d'un outil informatique permettant de protéger un système d'information, en filtrant les flux de données à destination ou en provenance d'un réseau, selon des règles définies par l'administrateur système.

Ce paramétrage doit être fonction du système et des besoins de la structure.

Il est impératif de protéger son réseau interne contre de potentielles intrusions en provenance de tout réseau public auquel il est susceptible d'être relié, et notamment Internet.

Pour les systèmes traitant de données sensibles, il est recommandé d'utiliser des réseaux dédiés.

2. Les antivirus

Ce logiciel informatique est essentiel pour protéger et préserver l'intégrité des données présentes sur un réseau ou sur les postes de travail contre tout type de virus (cf. lexique).

Même si aucun programme antivirus n'est parfait (les plus coûteux n'étant pas forcément les plus efficaces !), il convient *a minima* d'assurer des mises à jour régulières.

Cet outil de protection doit être présent sur chaque PC. Tout mail et document téléchargé à partir d'une source non fiable doit être soumis à divers contrôles, à commencer par un antivirus.

3. Les serveurs mandataires (*proxies*)

Un serveur *proxy* est un équipement faisant fonction d'intermédiaire entre le réseau local et Internet.

Il permet notamment :

- d'optimiser les performances d'Internet, en stockant la copie des pages souvent visitées (mémoire cache), en compressant les données, ou encore en filtrant certains contenus (publicités, contenus dits " lourds ") ou logiciels malveillants ;
- de contrôler les accès aux sites Internet non autorisés ;
- de journaliser les traces des sites visités ;
- d'assurer la sécurité du réseau local (visite de sites *Web* au travers d'une seule adresse IP) ;
- de garantir l'anonymat.

LE CHIFFREMENT

Le chiffrement est un procédé cryptographique permettant, en signant une information, d'en garantir la confidentialité, d'en assurer l'intégrité ainsi que l'authenticité.

Il s'agit d'empêcher la consultation en clair de données confidentielles. Cela peut également s'appliquer aux fichiers temporaires, aux historiques enregistrés par certains programmes, voire aux fichiers effacés.

Il est possible de chiffrer des supports (PC, supports mobiles, etc) mais également des fichiers ou un disque dur dans son ensemble – le chiffrement le plus large étant toujours la meilleure solution.

Les informations sont alors accessibles en saisissant une clé de chiffrement ou un mot de passe.

Il existe deux procédés cryptographiques :

- **la cryptographie symétrique**, par laquelle la même clé sert à chiffrer et déchiffrer. Ce système nécessite d'avoir autant de clés que de couples d'utilisateurs souhaitant communiquer en toute confidentialité ;
- **la cryptographie asymétrique**, qui utilise des clés différentes pour chiffrer (clé publique) et déchiffrer (clé privée). Ce système a pour avantage de supprimer la problématique relative à la transmission sécurisée de la clé.

L'utilisation de la cryptographie symétrique ou asymétrique est fonction des tâches à accomplir. Toutefois, les deux procédés se complètent.

Certaines solutions de chiffrement peuvent être configurées afin que les données soient automatiquement déchiffrées pour des utilisateurs autorisés.

Parmi les outils disponibles, des logiciels libres (cf. lexique) tels que *TrueCrypt6* (**www.truecrypt.org**) permettent de procéder au chiffrement des données dont la sécurité repose sur un mot de passe.

Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex. *smartphones*, ordinateurs portables, tablettes, etc), les données stockées et chiffrées doivent être effacées des supports mobiles sitôt qu'elles sont copiées dans le système d'information de la structure.

Les mesures de gestion des incidents

LA JOURNALISATION ET LA TRAÇABILITE

L'efficacité des mesures de sécurité proposées dans les rubriques précédentes ne serait pas optimale sans la mise en place d'un système de journalisation, permettant de retracer avec précision les divers évènements survenant au sein du système d'information.

En effet, l'obligation de sécurité du responsable de traitement implique également qu'en cas d'incident, celui-ci soit en mesure d'en comprendre l'origine et la cause, afin de prendre toute mesure rectificative nécessaire.

L'objectif premier est donc d'enregistrer à tout moment les traces (*logs*) laissées par l'utilisateur du système d'information : dates et heures de connexion - y compris les tentatives d'accès infructueuses au système ou à certaines ressources à accès restreint ; ressources sur lesquelles l'utilisateur s'est rendu (ex. dossiers, applications) ; type d'accès (en consultation, modification, suppression), etc.

Par ailleurs, le dispositif doit permettre d'identifier toute anomalie survenue sur le système d'information, notamment par l'établissement de *reportings* automatiques et réguliers. Ces journaux d'évènements peuvent disposer d'une durée de conservation programmée, ou fonctionner de manière cyclique, jusqu'à saturation de l'espace alloué, puis écrasement des données.

Selon l'organisation de la structure et la complexité de son système d'information, le dispositif de journalisation peut être centralisé. Dans cette hypothèse, les *logs* ne sont pas traités dans les applications dont ils sont issus (le cas échéant), mais dans un système distinct et identifiable, qui a pour seule finalité la traçabilité et la journalisation du système d'information.

Il en découle un traitement automatisé d'informations nominatives (adresse IP, identifiants de connexion, etc) ayant pour finalité *" Traçabilité et journalisation du système d'information "*. Sa mise en œuvre est soumise à une demande d'autorisation, conformément à l'article 11-1 de la loi n° 1.165, modifiée, considérant la nature intrinsèquement intrusive d'un tel système.

Dans les autres cas, les *logs* spécifiques à certaines applications (ex. messagerie, système de contrôle d'accès, vidéosurveillance, etc) sont générés dans des systèmes dédiés.

Il convient dans ce cas de considérer ces *logs* comme une catégorie de données parmi d'autres dans le cadre de traitements automatisés d'informations nominatives distincts (ex. Traitements ayant pour finalité *" Gestion de la messagerie "*, *" Contrôle d'accès par badge "* ou encore *" Sécurisation des locaux par vidéosurveillance "*).

Enfin, rappelons que pour qu'un tel système de journalisation soit opérationnel, il est indispensable que le système d'information dispose d'une horloge synchronisée avec une horloge de référence (serveur NTP : *Network Time Protocol*, ou SNTP : *Simple Network Time Protocol*).

LA SAUVEGARDE

La sauvegarde permet la prévention d'une perte accidentelle de données : mauvaise manipulation, incendie, panne matérielle, vol, etc.

Il convient de paramétrer :

- **le mode de sauvegarde :** la fréquence (ex. quotidienne), les versions à conserver, la méthode de sauvegarde (cf. lexique) (totale, incrémentale, décrémentale, différentielle, à delta, etc) ;
- **le support de sauvegarde et la destination** (ex. dans la structure ou à l'extérieur ; sur disque externe ou sur des équipements dédiés).

Il est impératif que le système de sauvegarde fasse l'objet de tests réguliers pour s'assurer de son bon fonctionnement.

Par ailleurs, une sécurisation renforcée sera requise pour la sauvegarde de données sensibles.

A cet égard, il est possible de chiffrer puis de compresser les sauvegardes, afin d'apporter une sécurité supplémentaire aux données, notamment lorsque celles-ci transitent sur Internet. Dans ce dernier cas, il convient de prévoir un chiffrement des données à la source.

Notons également que les données compressées transférées sur le réseau circulent plus rapidement, notamment lorsque la bande passante est limitée.

Pour les traitements revêtant des exigences fortes de disponibilité, il convient *a minima* de prévoir la connexion de l'infrastructure de télécommunication par deux voies différentes.

Une redondance matérielle des unités de stockage peut également être envisagée, par exemple via une technologie de type *" RAID "*, qui consiste à répartir les données sur plusieurs supports de sauvegarde (ex. disques durs) afin de prévenir la perte de données consécutive à la panne d'un des supports.

Enfin, afin de garantir la continuité de l'activité de la structure, l'utilisation d'un onduleur est fortement recommandée pour le matériel servant aux traitements indispensables.

Les accès distants, échanges de données, communications *Web* : VPN, SSL/SSH, HTTPS, FTPS

Un VPN (*Virtual Private Network*) est un réseau privé virtuel permettant de garantir la sécurité et la confidentialité des transferts d'informations pour toutes les applications utilisant Internet.

Les données chiffrées par l'expéditeur via des algorithmes de cryptographie et d'autres protocoles transitent dans un tunnel cloisonné au sein duquel aucune autre donnée ne peut entrer ou transiter, puis sont déchiffrées par le destinataire.

La mise en place d'un VPN nécessite l'installation d'un serveur VPN d'un côté (ex. au sein de l'entreprise), et d'un logiciel client VPN de l'autre (chez l'utilisateur itinérant).

L'utilisateur itinérant peut ainsi accéder à un réseau privé par le biais d'une connexion Internet.

Deux possibilités sont proposées :

- Solliciter le fournisseur d'accès Internet (FAI) ou équivalent : celui-ci établit une connexion chiffrée vers le serveur distant par le biais d'un *Network Access Server* du fournisseur d'accès, qui établira une connexion sécurisée.

  Cela implique toutefois que le serveur du FAI soit compatible avec la solution VPN choisie. En outre, la demande de connexion n'est pas chiffrée, ce qui peut poser des problèmes de sécurité.

- Détenir son propre logiciel client VPN et établir une connexion sécurisée (chiffrée) afin de communiquer vers le réseau de la structure.

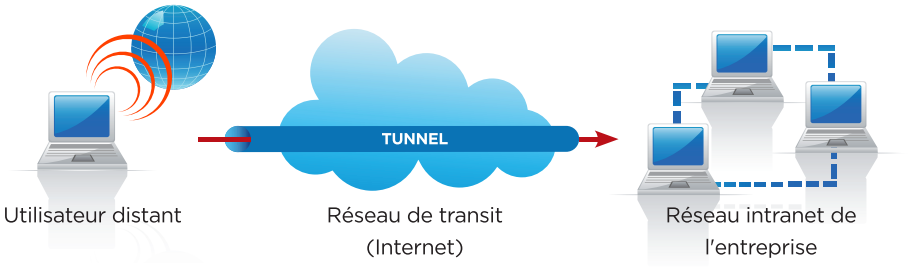
C'est la solution la plus répandue. Elle requiert néanmoins que le client ait à tout moment en sa possession le logiciel lui permettant d'établir ladite connexion.

LES TYPOLOGIES DE VPN

- Relier deux sites d'une même structure entre eux (ex. Intranet)

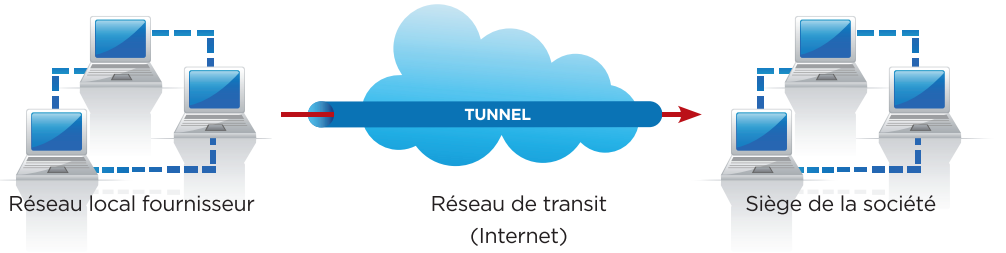
Ce type de VPN garantit la sécurité et l'intégrité des données échangées. Des techniques de cryptographie sont déployées afin de contrôler que les données n'ont subi aucune altération affectant leur validité. A cet effet, des algorithmes de signatures numériques sont ajoutés aux données transmises, assurant ainsi l'identification de leur source et leur non répudiation.

- Obtenir une connexion sécurisée avec des clients, des partenaires, etc



Il est impératif que l'administrateur informatique puisse tracer les clients VPN sur le réseau et gérer leurs droits d'accès. Cette traçabilité implique une collecte des *logs*.

- Réaliser des opérations de télémaintenance via des accès sécurisés (ex. SSH, *terminal serveur*)



LES METHODES DE CHIFFREMENT DES VPN

VPN chiffré grâce au protocole IPSec (*Internet Protocol Security*)

IPSec fournit un ensemble de services de sécurité en permettant à un système de choisir les protocoles de sécurité requis, de déterminer l'algorithme à employer pour le service concerné, et d'établir les clés de chiffrement requises pour assurer les services demandés.

Aujourd'hui, IPSec est l'un des moyens les plus sécurisés pour accéder à un réseau informatique via Internet, ou encore pour effectuer des transactions sur le Web. L'architecture IPSec est décrite dans la RFC 2401 (http://www.ietf.org/rfc/rfc2401.txt).

VPN chiffré grâce au protocole SSL (*Secure Socket Layer*)

Le protocole de sécurisation des communications Internet SSL, aussi connu sous le nom de TLS, est l'un des standards les mieux reconnus, au travers du système d'adressage " *https://* " (HTTP sécurisé par SSL) et d'autres protocoles comme SMTP (pour les messageries).

Ex. Un cadenas verrouillé indique que la connexion à un site est sécurisée par SSL et un cadenas ouvert indique le contraire. Lorsqu'aucun cadenas n'apparaît, c'est qu'il existe des doutes quant à la sécurisation de la connexion.

Ce protocole permet d'obtenir une connexion Internet sécurisée grâce à un chiffrement des données échangées entre un PC et un serveur authentifié. L'authentification est proposée côté client par l'échange d'une clé publique.

Le protocole SSL est toujours utilisé pour des sites Internet permettant des opérations bancaires ou commerciales, car les clients accèdent souvent à ces sites par le biais du réseau Internet public.

Enfin, SSL est également utile lors d'un échange entre deux applications.

VPN chiffré grâce au protocole SSH (*Secure Shell*)

Ce protocole fournit une double sécurisation qui consiste à prendre en charge l'authentification serveur/utilisateur, ainsi qu'à chiffrer l'ensemble des données échangées entre le client et le serveur. Il crée un tunnel entre deux applications, qui reste ouvert et disponible.

Il permet ainsi :

- de disposer de sessions actives en mode Telnet ;
- d'effectuer des transferts de fichiers sécurisés ;
- d'exécuter des commandes à distance sécurisées.

SSH est généralement utilisé pour la sécurisation de protocoles tels que : FTP, POP3/ IMAP/ SMTP, Telnet, etc.

La différence entre SSL et SSH porte essentiellement sur les mécanismes d'authentification client/serveur intégrés dans les protocoles.

Le protocole FTPS (*File Transfer Protocole* sécurisé par SSL)

Il s'agit d'un protocole de transfert de fichiers qui permet de définir les paramètres de transmission de données sur un réseau. Pour sa sécurisation, il utilise le protocole SSL.

Ainsi, il est possible de copier des fichiers d'un PC à un autre, d'alimenter un site Internet, ou encore de supprimer ou modifier des fichiers d'un PC.

Quelques mots sur les *cookies*...

Un " *cookie* " est un petit lot d'informations stocké par un navigateur Internet. Il se localise sur le disque dur d'un internaute, dès lors que ce dernier navigue sur un site, et permet d'enregistrer les informations relatives à l'internaute (adresse IP, informations techniques relatives au PC, historique de navigation, etc).

Il existe plusieurs types de *cookies* :

- certains ont simplement une finalité technique, ou sont nécessaires à l'ergonomie de la navigation : ex. les *cookies* des messageries Internet telles que *Hotmail* ;
- d'autres ont un objectif de profilage, à des fins commerciales ou de publicité : ex. les *cookies* qui tracent les articles consultés sur un site de vente en ligne et permettent l'affichage de ces derniers dans des encarts publicitaires lorsque l'utilisateur bascule vers un autre site.

Les *cookies* représentent un risque pour les données personnelles car ils permettent l'enregistrement de nombreuses informations, à commencer par les identifiants et mots de passe.

Ainsi, il convient *a minima* de configurer le navigateur Internet pour empêcher autant que possible la collecte de ces données. Par ailleurs, certains logiciels tels que *Gosthery* (logiciel gratuit) permettent d'empêcher la collecte des traces de navigation sur Internet.

Les appareils mobiles en bref...

La naissance de nouvelles technologies telles que les tablettes (Wifi, 3G, IP) ainsi que la transformation des téléphones portables en téléphones intelligents (Wifi, IP, 3G, 3G+, 4G) ont entrainé l'apparition de nouveaux virus, adaptés à ces nouvelles conceptions informatiques.

Ces virus ou *malwares* développés pour des terminaux mobiles sont comparables à ceux développés pour les PC. Ils peuvent infecter tout un système, corrompre ou écraser des fichiers, espionner les activités de l'utilisateur, envoyer des SMS surtaxés, bloquer le terminal.

Une connexion de l'appareil mobile infecté au système d'information peut également mettre en péril l'intégrité de ce dernier.

Ces attaques implémentées par des agents malveillants via, par exemple, un téléchargement Internet sur le mobile, peuvent perturber les fonctions de l'appareil afin de :

- manipuler les données (attaques d'intégrité) ;
- relever des informations personnelles, des codes d'accès (applications bancaires, commerce électronique, réseaux sociaux).

Ainsi, les exigences minimales de sécurité pour ces équipements sont, notamment :

- l'authentification des utilisateurs ;
- l'application d'antivirus ;
- la sécurisation de l'accès réseau (le VPN est applicable aux appareils mobiles) ;
- la sécurisation des communications ;
- la sécurisation de la carte mémoire (chiffrement) ;
- le contrôle du téléchargement (applications autorisées).

POUR RESUMER :

LES PRATIQUES RECOMMANDEES POUR LA SECURITE DES RESEAUX

Nombreuses sont les solutions existantes en matière de sécurité. Mais aucune ne garantit une sécurité sans faille. Tout est une question de bon sens et de cumul de solutions.

« LE MOT D'ORDRE EST : REDUIRE LES RISQUES ! »

Voici en résumé les mesures à prendre impérativement en considération :

- utilisation et mise à jour de logiciels antivirus et anti-espions gérés de manière centralisée sur tous les hôtes du réseau ;
- mise en place de *firewall* (pare-feu) sur tous les segments du réseau (privé et public) avec des règles de *firewall* déployées de manière centralisée ;
- gestion et verrouillage des ports inutiles du réseau ;
- authentification sécurisée et centralisée (ex. *Active Directory*, *Radius*, etc) ;
- gestion centralisée des habilitations ;
- chiffrement des connexions Internet (VPN, SSL, etc) ;
- chiffrement de tous les supports mobiles (clé USB, portables, téléphones mobiles, CD, etc) destinés à recevoir des informations à caractère personnel ;
- analyse et surveillance des comportements suspects sur le réseau (traçabilité des *logs*, etc) ;
- remontée automatique et centralisée de tout incident technique ;
- mise en place d'une charte informatique.

Si vous pensez que la technique peut résoudre tous vos problèmes de sécurité, c'est que vous n'avez rien compris à la technique, ni à vos problèmes.
Bruce Schneier, expert en chiffrement et sécurité informatique.

LEXIQUE

- Adresse IP (*Internet Protocol*)
  Identifiant unique attribué à tout ordinateur sur le réseau. Pour les particuliers, l'adresse IP est fournie par le fournisseur d'accès internet (FAI).
  Elle peut être attribuée de manière permanente (IP statique) ou bien plus généralement à la volée (IP dynamique).

- Information nominative
  " *[Information] qui permet d'identifier une personne physique déterminée ou déterminable. Est réputée déterminable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propre à son identité physique, physiologique, psychique, économique, culturelle ou sociale* " (art. 1er al. 2 de la loi n° 1.165).

- Intranet (Réseaux privés d'entreprise)
  Réseau local et privé utilisant la même technologie et les mêmes protocoles qu'Internet, généralement limité à une entreprise et qui ne s'ouvre pas aux connexions publiques, contrairement à Internet.

- Logiciel libre
  Logiciel qui peut être librement utilisé, étudié, modifié et redistribué.

- Méthodes de sauvegarde
  La sauvegarde est dite " *totale* " lorsque l'ensemble des données est copié sur un support distinct.

  Elle est " *différentielle* ", lorsque ne sont enregistrés que les fichiers modifiés depuis la dernière sauvegarde totale. Pour reconstituer l'ensemble des données, il convient donc de rapprocher la sauvegarde totale et la sauvegarde différentielle.

  La sauvegarde est dite " *incrémentale* " lorsque sont enregistrées les données modifiées depuis la dernière sauvegarde (qui n'est pas forcément une sauvegarde totale). Rapide et performante, ce type de sauvegarde nécessite toutefois de conserver toutes les précédentes sauvegardes afin de reconstituer l'ensemble des données.

- Responsable de traitement
  Personne physique ou morale, de droit privé ou de droit public, autorité publique, service ou tout autre organisme qui détermine, seul ou conjointement avec d'autres, la finalité et les moyens du traitement et qui décide de sa mise en œuvre (art. 1er al. 4 de la loi n° 1.165).

- Traitement d'informations nominatives
  " Toute opération ou ensemble d'opérations portant sur [des informations nominatives], quel que soit le procédé utilisé. Celles-ci portent sur la collecte, l'enregistrement, l'organisation, la modification, la conservation, l'extraction, la consultation ou la destruction d'informations, ainsi que sur l'exploitation, l'interconnexion ou le rapprochement, la communication d'informations par transmission, diffusion ou toute autre forme de mise à disposition " (art. 1er al. 3 de la loi n° 1.165).

- Virus informatique
  Programme informatique créé dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés *" hôtes "*. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet mais aussi les CD, les clés USB, etc.

“ LES SITES *" SECURITE INFORMATIQUE "* PRECONISES ”

Sécuriser son système informationnel ne nécessite pas nécessairement de gros investissements financiers. Certains logiciels gratuits tout aussi efficaces peuvent être téléchargés, par exemple, sur les sites suivants :

- **(http://www.truecrypt.org)**
- **(http://www.secuser.com)**
- **(http://www.clubic.com)**
- **(http://www.inoculer.com)**
- **(http://urlquery.net)**
- **(http://www.pcastuces.com/pratique/securite)**
- **(http://www.piriform.com/download)**

Article 17 de la loi n° 1.165, modifiée :

" Le responsable de traitement (...) est tenu de prévoir des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Les mesures mises en œuvre doivent assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger.

Lorsque le responsable de traitement (...) a recours aux services d'un ou plusieurs prestataires, il doit s'assurer que ces derniers sont en mesure de satisfaire aux obligations prescrites aux deux alinéas précédents (...) ".

Commission de Contrôle
des Informations Nominatives

12 AVENUE DE FONTVIEILLE
98000 MONACO

TÉL. : +377 97 70 22 44 – FAX. : +377 97 70 22 45

CCIN@CCIN.MC – WWW.CCIN.MC