La sécurité des traitements : une approche globale

Aux termes de l'article 17 de la loi n° 1.165 du 23 décembre 1993 :

« *Le responsable du traitement ou son représentant 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 autorisés, 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 du traitement ou son représentant 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 précédents alinéas.

La réalisation de traitements par un prestataire doit être régie par un contrat écrit entre le prestataire et le responsable du traitement ou son représentant qui stipule notamment que le prestataire et les membres de son personnel n'agissent que sur la seule instruction du responsable du traitement ou de son représentant et que les obligations visées aux deux premiers alinéas du présent article lui incombent également.

Si le prestataire souhaite avoir recours aux services d'un ou de plusieurs sous-traitants pour l'exécution de tout ou partie des prestations prévues au contrat susvisé, les dispositions de l'alinéa précédent s'appliquent à ces derniers ».

Cette obligation de préservation des données à caractère personnel figure également à l'article 32 du RGPD.

La nécessité de protection des informations nominatives concerne tant les fichiers au format papier que ceux au format numérique.

Que veulent savoir les techniciens lors d'une analyse de dossier ?

Comment les techniciens analysent la sécurité d'un dossier ?
C'est une question que beaucoup de responsables de traitement se posent. S'il n'y a pas de formule clé en main, 6 étapes peuvent néanmoins être identifiées.

I. Etapes de l'analyse

1/ Les techniciens s'intéressent tout d'abord à la finalité du traitement qui amène à connaitre le type de données collectées. Le **cycle de vie des données** (flux) permet d'avoir des indications à la fois sur la donnée elle-même ainsi que sur son exploitation.

2/ Ils étudient ensuite les habilitations octroyées et la traçabilité (imputabilité possible des actions). Le **schéma d'architecture technique** a son importance car il aide à la compréhension du système technique déployé.

3/ Puis vient la sécurité appliquée aux données au regard de la finalité, à savoir :

- les données identifiantes, pseudonymisées, anonymisées, etc. ;
- la localisation des données : stockage interne, hébergement, cloud, etc. ;
- la sécurité logique et physique ;
- le chiffrement mis en place ;
- les sauvegardes et leurs localisations ;
- etc.

4/ La communication des données est également étudiée, comme par exemple :

- via les portails web ;
- par le biais d'une messagerie électronique ;
- par le biais de support(s) physique(s) (clé USB, disque dur, etc.) ;
- etc.

5/ Sans oublier, lorsque cela est le cas, tout transfert[1] de données vers un pays hors protection adéquate, avec la sécurité des données concernées par ce transfert.

6/ Enfin, il est important pour les techniciens de savoir avec quel(s) autre(s) traitement(s) le traitement étudié est rapproché et/ou interconnecté. Une justification de ce(s) rapprochements(s)/interconnexion(s) doit être fournie.

II. Cas pratique

Une entreprise sise à Monaco dépose un dossier portant sur la vidéosurveillance dont le prestataire de Télésurveillance est situé en Italie.

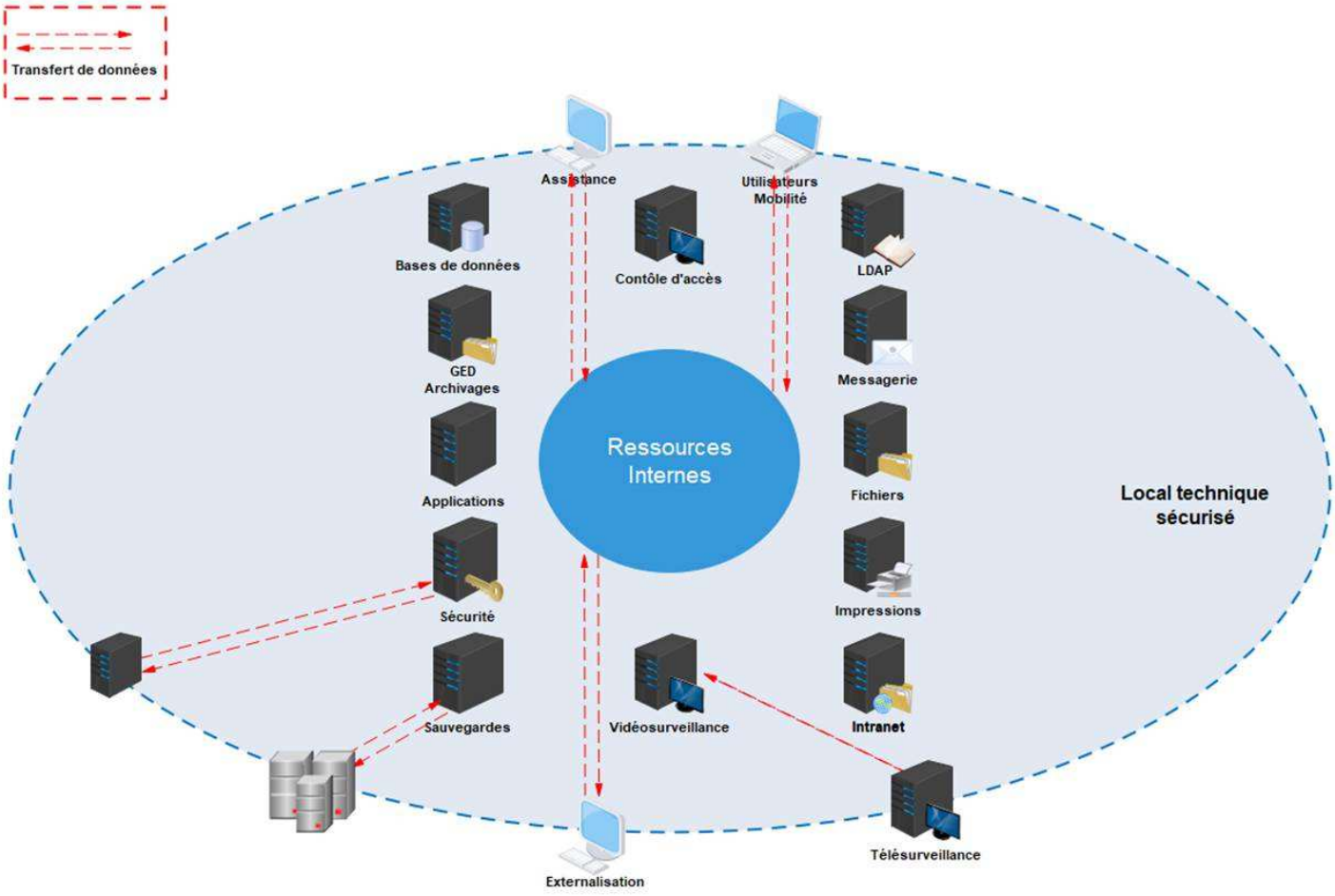
Documents fournis :

- le formulaire de demande d'autorisation complété ;
- le schéma d'architecture technique (flux des données) ;
- le plan d'implantation des caméras.

Pour tout traitement soumis à autorisation/avis, les techniciens rédigent un rapport technique relatif à la sécurité dudit traitement. Ce rapport est présenté en Commission afin d'aider à la compréhension technique de ce traitement et à la prise de décision.

[1] Sont également considérés comme des transferts, **les accès** aux informations effectués depuis un pays ne disposant pas d'un niveau de protection adéquat.

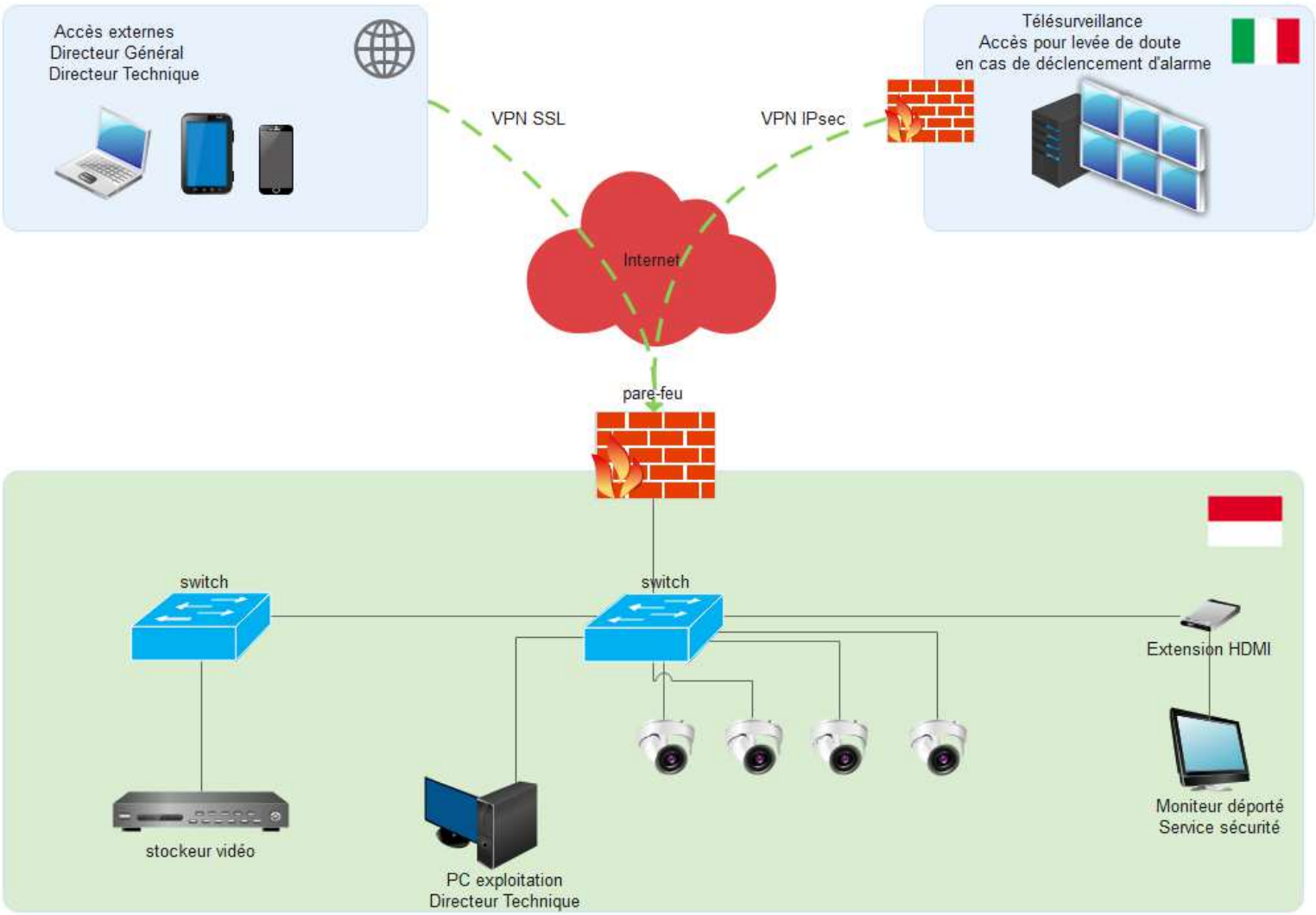
Schéma d'architecture technique globale de l'entreprise sise à Monaco



Le schéma d'architecture globale fourni par l'entreprise permet d'avoir une vision générale sur l'infrastructure technique.

Cependant, afin de comprendre le traitement concerné, les techniciens ont besoin d'avoir un schéma plus précis identifiant dans cette structure ledit traitement, en l'espèce, le dispositif de vidéosurveillance.

Focus sur le schéma d'architecture technique du traitement de vidéosurveillance



1/ Conformément à la procédure décrite dans la partie I, les techniciens se penchent d'abord sur la finalité qui consiste en l'installation d'un système de vidéosurveillance à des fins sécuritaires. Les quatre caméras installées sont fixes et les fonctionnalités zoom et micro ne sont pas activées. Seuls sont ainsi collectés les images, visages et silhouettes des personnes.

2/ Les techniciens analysent les habilitations ainsi que les différents types d'accès. Le schéma d'architecture technique du traitement permet notamment de vérifier la cohérence des habilitations indiquées et met aussi en évidence des accès distants sécurisés (VPN SSL) par des personnes internes à l'entreprise (le Directeur Général et le Directeur Technique).

3/ Sur la sécurité du traitement, les techniciens constatent les points suivants :

- le stockeur vidéo se situe dans un local technique fermé à clé ;

- il y a un moniteur déporté ;
- chaque personne habilitée dispose d'un identifiant et d'un mot de passe individuels pour accéder au traitement ;
- une journalisation des accès est mise en place ;
- etc.

Ils vérifient également à l'aide du plan d'implantation, l'angle de vue des caméras et, quand elles sont fournies, les captures d'écran.

4/ Les techniciens notent que l'extraction des images s'effectue sur une clé USB. Toutefois aucune procédure de chiffrement n'est prévue. Dans leur rapport technique, les techniciens demandent donc que l'extraction des images soit impérativement chiffrée sur son support de réception.

5/ A l'étude du dossier les techniciens constatent qu'il n'y a aucun transfert vers un pays hors protection adéquate. Cependant ils relèvent qu'en cas de déclenchement d'alarme, un accès aux images depuis l'Italie est effectué par le prestataire de Télésurveillance.

6/ Le responsable indique que le traitement ne fait l'objet d'aucun rapprochement ni d'interconnexion avec un autre traitement. Cependant, à l'analyse du schéma d'architecture technique, les techniciens relèvent que le prestataire de Télésurveillance agit uniquement sur déclenchement d'alarme. Il y a donc une interconnexion liée à ladite alarme qui doit être déclarée auprès de la CCIN.

Du pare-feu à l'extincteur ou de l'importance de la sécurité physique des locaux hébergeant des informations nominatives

Souvent, surtout concernant les données conservées par le biais d'un système informatique, la notion de sécurité et de conservation n'est envisagée que du point de vue strictement informatique par l'installation de divers outils (exemples pare-feu, anti-virus, chiffrement, hachage, …).

Cependant, la sécurité des données ne se limite pas à ces aspects et doit être pensée de manière globale. Il est en effet inutile d'avoir un système sophistiqué destiné à prévenir les intrusions à distance dans un système d'information s'il est possible d'ouvrir facilement le local où se trouve le serveur informatique et de s'y connecter directement.

Lors de l'élaboration d'un plan de sécurité, la sécurisation des différents locaux est indispensable et doit être adaptée à l'entreprise et à son activité.

Il convient d'analyser les risques (externes, internes, humains, naturels, …), leur vraisemblance (c'est-à-dire la probabilité qu'ils surviennent), la gravité de leurs conséquences éventuelles, les manières de les prévenir et si besoin de remédier à leurs effets néfastes.

Ces risques peuvent être reportés sur une cartographie des risques, et ne seront pas les mêmes selon par exemple que l'on se trouve dans un immeuble collectif divisé entre plusieurs entités ou dans un immeuble n'abritant que l'entreprise notamment en ce qui concerne la gestion des accès à l'intérieur de cet immeuble ou selon que l'entreprise reçoit ou non du public.

Un immeuble ancien ou même neuf peut ne pas avoir été conçu pour abriter tel type de société car n'offrant pas les garanties nécessaires de sécurité active et passive.

Un audit de sécurité ne doit pas négliger le volet de la protection physique des installations et le recours à un prestataire spécialisé peut être nécessaire. Dans certains cas, le recours à des *bug bounty* ou hackers éthiques peut permettre de tester la sécurité à *« 360° ».*

De manière générale, il convient de s'assurer que l'accès aux locaux est sécurisé au moyen d'alarmes, de caméras et d'un contrôle d'accès par badge par exemple. Différentes zones doivent être définies en fonction de leur sensibilité aux risques.

Les locaux eux-mêmes doivent être conformes à la sensibilité de l'usage et au risque d'intrusion par exemple par la sécurisation des murs, fenêtres et portes d'entrée. Les accès secondaires ne doivent pas être négligés (par exemple à partir de la cave, du parking, d'un local voisin, …).

La sécurité doit également prendre en compte outre les risques extérieurs humains, les risques naturels par des protections contre les incendies ou les dégâts des eaux, les pannes électriques, …

Ainsi, le local abritant les serveurs informatiques, cœur de la protection informatique et par conséquent zone à haut risque d'intrusion et d'action malveillante possible, doit faire l'objet d'une attention particulière. Il doit être installé dans un lieu sécurisé anti-incendie et limitant le risque de dégâts des eaux, être correctement climatisé (il ne sert à rien d'en contrôler l'accès si on laisse la porte ouverte pour refroidir en aérant), muni d'un onduleur et maintenu dégagé de tout élément pouvant en compromettre la sécurité (on n'y entrepose pas de cartons par exemple ou de produit inflammable).

Son accès ne doit être autorisé qu'aux personnes dont la fonction implique nécessairement d'y entrer et toute personne extérieure même un prestataire lié à l'entreprise par un contrat doit y être accompagné par une personne habilitée de l'entreprise. Des badges d'accès ou des contrôles d'accès biométriques ainsi que des caméras peuvent être utilisés. Les accès doivent être tracés sur un registre même pour les personnels de l'entreprise. En cas d'intervention, la nature et la durée doivent y figurer.

Par analogie, au principe du « *besoin d'en connaître* » bien connu en matière de protection des informations nominatives, les accès aux différentes zones de l'entreprise doivent être fondés sur le « *besoin d'y accéder* ». Ainsi, un employé qui

n'aurait qu'un besoin ponctuel d'accès n'a pas lieu de bénéficier d'un droit d'accès permanent et l'hôtesse d'accueil n'a pas vocation à entrer dans la salle des serveurs informatiques par exemple.

Pour les zones moins sensibles, des accès plus libres peuvent être mis en place. Cependant, une attention particulière est nécessaire afin de prévenir la circulation de personnes extérieures qui pourront par exemple être tenues de porter un badge visiteur apparent.

Un registre des visites peut être établi. Une attention particulière sera portée aux livreurs et autres prestataires qui pourraient être amenés à circuler dans les lieux.

Dans les zones non soumises à un contrôle d'accès strict, les ordinateurs fixes ou portables doivent faire l'objet de mesures de sécurité afin d'empêcher d'y accéder ou de les emporter (par exemple par l'utilisation de câbles anti-vols). Seul le matériel fourni par l'entreprise doit pouvoir être connecté au réseau de l'entreprise et les outils nomades comme les clefs USB doivent être protégés notamment du vol et chiffrés afin de réduire le risque si cela devait survenir.

Le personnel doit être sensibilité régulièrement à la sécurité globale et aux bonnes pratiques. Son attention doit être appelée sur les risques liés aux objets connectés personnels et à l'usage d'outils personnels qui peuvent être des vecteurs d'entrée de risques ou d'intrusion.

Les sauvegardes informatiques doivent être stockées dans des locaux distincts des locaux principaux. Les supports physiques de ces sauvegardes ou les documents papier sensibles doivent être placés dans des coffres forts ignifugés et étanches.

Les documents sensibles ne doivent pas être laissés sur les bureaux en dehors de la présence des personnes qui les occupent. Les open-space et les espaces de bureaux partagés nécessitent une attention et une rigueur particulière.

La gestion des codes d'accès doit faire l'objet d'une revue périodique et être régulièrement mise à jour afin notamment de priver rapidement d'accès un salarié qui quitterait l'entreprise.

Tous les intervenants extérieurs doivent être gérés selon le risque afin de prévenir tout acte malveillant.

Les copieurs multifonctions doivent également être protégés car ils stockent un grand nombre d'informations.

Les écrans affichant des données sensibles ne doivent pas être visibles de l'extérieur ou du public.

Les documents devenus inutiles mais pouvant contenir des informations sensibles doivent faire l'objet d'une destruction répondant aux normes en vigueur afin de prévenir leur reconstitution. L'inspection de vos poubelles peut en dire beaucoup sur votre entreprise et son activité.

Si vos données sont hébergées par un prestataire extérieur ou un sous-traitant, il vous appartient de vous enquérir des mesures de sécurité qu'il applique à ses locaux pour

réduire le risque de divulgation ou de compromission susceptible d'engager votre responsabilité.

La sécurité commence par l'anticipation et le bon sens de chacun (comme en médecine *« mieux vaut prévenir que guérir »*) et est l'affaire de tous.

Des failles de sécurité même d'apparence mineure peuvent exposer à des conséquences dramatiques tant pour la société que pour les personnes dont les données auront été piratées.