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, etc.).

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.

Analyse des risques

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, etc.), 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° ».*

Sécurisation des accès

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, etc.).

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, etc.

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 données personnelles, 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.

Sécurité interne

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.