GÉRER LES RISQUES QU'UN TRAITEMENT FAIT PESER SUR LES PERSONNES CONCERNÉES

Métier : Médecine du travail

Le système d'information d'un service de médecine du travail est sensible, au même titre que ceux des autres cabinets médicaux. Leur sécurisation doit cependant respecter une enveloppe de coûts raisonnable et cibler les risques prioritaires. Ceux-ci peuvent être définis comme ceux relevant de la conformité réglementaire et ceux dont la vraisemblance est la plus importante.

Pour déterminer les risques sur lesquels concentrer l'investissement de sécurité, l'application d'une méthodologie rationnelle et reconnue apporte une solution crédible. En France deux grandes méthodologies sont disponibles gratuitement et reconnues dans les entreprises et administrations. La présente analyse a utilisé EBIOS, publiée par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

QUE DOIT-ON ANALYSER ?

Il s'agit d'un petit service de quatre personnes suivant 400 salariés, utilisant un logiciel du marché.

L'analyse met en évidence les **éléments à protéger** et leurs **supports** :
- données à caractère personnel : identité des salariés, données relatives à la santé ;
- processus légaux : information, consentement, droits d'accès, d'opposition et de rectification ;
- supports : ordinateurs, réseau, locaux, logiciel métier, système d'exploitation.

Le **cadre réglementaire** et contractuel de l'activité est constitué des Codes de la Santé et Pénal, de la Loi Informatique et Libertés, des recommandations de la Haute Autorité de Santé, et des contrats liant le cabinet à ses fournisseurs.

Les principales **sources de risques** sont sélectionnées pour leur probabilité : vol d'information, virus, pannes, erreurs d'utilisations, etc.

Les **mesures de protection existantes** sont répertoriées pour modérer le risque réel encouru.

QUELS SONT LES RISQUES ?

L'hypothèse d'un sinistre est estimée à partir de la confrontation des éléments collectés dans l'analyse, puis sa vraisemblance est calculée afin de dégager les risques les plus urgents à traiter.
Les principaux risques à couvrir sont :

- **l'accès illégitime aux données** (virus, agent interne, tiers externe) : ces informations pourraient être exploitées pour nuire aux salariés concernés, la responsabilité du service de Médecine du travail serait engagée au regard de plusieurs lois. Les conséquences pourraient être pénales, financières et de réputation ;

- **la modification non désirée de données** ou **des processus légaux** (accidentelle ou malveillante) aurait un impact de réputation et de surcoût lié à la remise en état du système.

QUELLES SOLUTIONS ?

Les solutions sont particulières à chaque situation dans leur intensité ou l'étendue de leur application, le coût y étant souvent proportionnel. L'analyse a conduit à distinguer les solutions les mieux à même de couvrir les principaux risques.

La protection des données et des processus légaux passe par plusieurs mesures :
- la maintenance et les tiers ne doivent pas avoir accès à l'information. Un système dont l'information sera anonymisée en interne (la base de données) sera plus sûr lors de la maintenance ou en cas de vol. A défaut, un suivi nominatif des techniciens habilités et des clauses contractuelles établissent un transfert de responsabilité vers la société de maintenance.
- le **contrôle des accès** aux locaux et à l'application doit être rigoureux. Des systèmes par carte (ex : CPx) garantissent au mieux ce contrôle. Si ces dispositifs ne sont pas disponibles, des mots de passe de bonne qualité, renouvelés régulièrement et une **traçabilité** exploitable des accès et des modifications permettent de réduire le risque de sinistre.

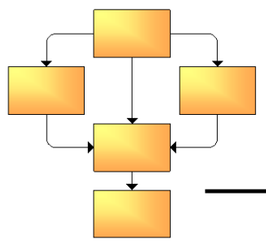
La **conformité aux réglementations** passe par une prise de connaissance des obligations et la sensibilisation des utilisateurs du système :
- la finalité de l'activité (ici la médecine du travail) ne doit pas être détournée ;
- le besoin d'accéder à l'information concernant un individu doit être justifié non seulement par la fonction de l'utilisateur, mais aussi par sa mission ponctuelle ;
- les personnes répertoriées par le système ont un droit d'accès et de rectification garanti par la loi, il faut l'organiser par une procédure dans la durée.

Le choix des solutions permet de réduire les risques afin que ceux qui persisteront deviennent acceptables pour le propriétaire et l'organisation : leur réalisation sous la forme d'un sinistre ne fera pas obstacle à la pérennité du service ou des professionnels qui le compose.

CONCLUSION

L'analyse rationnelle des risques permet de limiter l'investissement aux éléments à protéger et aux risques les plus graves et les plus vraisemblables. Elle doit également se contraindre elle-même à cibler les priorités dans un temps contraint, sans tomber dans la répétition d'un schéma convenu à l'avance : chaque métier est particulier par sa réglementation, son lieu d'activité, ou les modalités de sa production.

La méthodologie de gestion des risques est une démarche simple et documentée qui permet d'extraire les principaux risques d'un système en maîtrisant le niveau de détail.



Club EBIOS