NOUVELLES TECHNOLOGIES

PAR J.F. COBLENTZ

Protection des données en santé : bien se protéger en tant que professionnel !

Ça ne vous viendrait à pas l'esprit de laisser le dossier d'un de vos patients sur un banc public… Ce même bon sens doit s'appliquer sur vos données non physiques ! Il est délicat (euphémisme) de devoir annoncer à un patient la perte totale et irréversible de son dossier ou la fuite de ses données entrées dans votre système d'informatique vers des contrées inconnues. L'idée vous rend mal à l'aise ? On vous comprend ! Hors, ce risque est minimisable.

Pourquoi renforcer la sûreté de votre système informatique ?

La question parait basique mais … Savez-vous exactement à quels risques sont exposés vos matériels et vos données informatiques ? Tout comme il est primordial de connaître son ennemi pour mieux le combattre, il est important de classifier les risques pour être à même de prendre les mesures préventives adéquates :

- cambriolage / vol,
- virus,
- sinistre (électrique, inondation, incendie …),
- erreur humaine de manipulation,
- panne matérielle / dysfonctionnement.

La perte ou la destruction de vos matériels et/ou de vos données peut avoir des conséquences importantes : arrêt d'activité, pertes financières, préjudice d'image pour le cabinet… Quelques secondes suffisent pour perdre plusieurs années de travail.

Précisons que l'auteur de ces lignes a été récemment traité d'extrémiste pour tenir un discours de préservation "à tous prix" des données de santé.

Des mesures simples et efficaces à adopter

Pour vous prémunir contre ces diverses mésaventures, des mesures simples, mais qui ont fait leurs preuves, sont à mettre en place :

- limiter l'accès aux postes et aux données à un nombre limité

de personnes pour diminuer les risques d'erreur humaine ou de piratage ;

• sécuriser physiquement vos équipements « *sensibles* » (serveur, box, par exemple) dans une ou des pièces fermées à clé et/ou équipé d'une alarme,

• restreindre les accès logiciels avec des mots de passe « *forts* »,

• se protéger des virus grâce à des anti-virus performants ET A JOUR,

• confier si besoin votre sécurité informatique à un prestataire externe,

• maintenir à jour vos logiciels,

• sensibiliser votre équipe aux bonnes pratiques pour réduire les risques de piratage.

Figure 1 : se protéger, point essentiel

Quels outils ?

Le nombre d'attaques de pirates a considérablement augmenté (certains de vos confrères l'ont vécu assez douloureusement), et le défi à relever, en matière de sécurisation des données, est important. Bien sûr, il y a des solutions de sécurité de prévention. Votre rôle est primordial et vous ne pouvez vous dérober.

Figure 2 : prêter attention à son environnement

Figure 3 : Aucune solution n'est fiable à 100%

Passons ici (nous y reviendrons dans un autre article) sur les risques liés aux intrusions (Figure 3), ceux liés aux évaluations des taux de panne (promesse identique). Nous partons du principe que, tout de même, vous réalisez des sauvegardes quotidiennes de vos données (logiciel de gestion, logiciels 3D et radio, mails professionnels, …). Il est maintenant reconnu que cela ne suffit pas à une sécurité complète. Pour y tendre, il est indispensable de réaliser des sauvegardes soit sur un système réparti (RAID - Figure 4), soit sur des supports multiples (par exemple en alternant un jour sur deux), soit enfin, et avec des précautions qui seront évoquées plus loin, réaliser en plus une sauvegarde sur un Cloud (de vous même ou par un prestataire).

Figure 4 : Système RAID

Traditionnellement on considère que la mesure de sécurité que vous pouvez évaluer est fondée sur un principe simple : quelle durée de données est-il acceptable de perdre, statistiquement ? Selon votre réponse, les solutions et leur mise en œuvre seront différentes. Ainsi, accepter de perdre 1 heure ou 3 jours ne correspondent pas aux mêmes outils. Nous suggérons de positionner la bonne mesure à 1 demi-journée.

A noter que le terme "statistiquement" est important. En effet, perdre une demi-journée 'statistiquement' signifie que le risque de perte est compris entre 0 et 1 journée.

La moindre des choses est de disposer de deux supports et de les alterner pour, en permanence, en avoir un à l'extérieur du cabinet. En les échangeant chaque jour, vous laissez la

sauvegarde se faire de nuit et disposez ainsi des données de la veille en cas de besoin immédiat. Perte moyenne "statistique": 1 demi-journée ! CQFD.

Cette solution, simple, est sans doute un peu légère mais a fait ses preuves. En effet, laisser les sauvegardes dans le cabinet sans jamais en sortir ne répond pas aux deux problèmes que sont les vols et les risques naturels, de type incendie. Ou alors, nous pouvons suggérer de compléter cette solution insuffisante par un abonnement de sauvegarde en ligne. N'oubliez jamais que la sauvegarde en ligne doit être testée pour vérifier le temps réel de mise à disposition des données lorsque le besoin surgit. L'orthodontie manipule des volumes de données très importants. Les temps de transfert sont à cette aune. Par ailleurs, en cas de recours à ce type de sauvegarde, soyez prêts et réfléchissez aux données dont vous avez besoin le plus rapidement et celles qui peuvent revenir un peu plus tard (dossiers activés, photos de plus de x années, …).

Un tour d'horizon rapide

Les solutions accessibles sont devenues innombrables. Il devient difficile de mépriser les risques au prétexte de complexité. De la clé USB à la sauvegarde en ligne, en passant par les NAS, tout est devenu accessible techniquement et financièrement.

Le support USB amovible : clé, disque, … sont des outils très peu coûteux. Nous aimons moins les clés car les précautions prises avec sont moindres, tant leur format, lui même, les rend à risque (perte, chute, casse, …). Des disques durs "de poche' nous semblent plus sérieux. Vous pouvez en avoir autant que nécessaire pour assurer votre schéma de sécurité. Nous aimons bien l'idée d'en avoir plusieurs comme, par exemple, un par jour de travail. Une solution comme une autre, simple à mettre en œuvre. Le support du jour est au cabinet (comme celui de la veille car il n'est pas encore sorti). Le soir, la personne en charge part avec la sauvegarde de la veille et laisse celle du jour.

La sauvegarde sur le réseau du cabinet est une autre solution, simple et économique. Notons toutefois que des sauvegardes de ce type ne devraient pas être réalisées pendant les heures de travail, pour des raisons de sécurité des données (copier des fichiers ouverts ou en cours de fonctionnement n'est jamais très sûr) comme pour des raisons de performances (charge du réseau). Une suggestion : planifier de telles sauvegardes midi et soir si le cabinet interrompt le travail le midi. On en arrive alors à un risque statistique de 3 à 4 heures maxi. Mais cette solution ne retire pas le besoin de sortir les données.

Mais, il ne faut jamais oublier que les esprits chagrins veillent, hélas. Par exemple, le 'ransonware' Wooxo, s'installe sur des supports USB externes et attend quelques jours pour tout bloquer, machines et supports USB. C'est là que les solutions par disque externe ou vers un Cloud deviennent

Figure 5 : Un simple disque est un élément de la solution (non numérotée dans l'article)

complémentaires. Comprenez bien que toute solution à ses revers, presque toujours en raison de malveillances sans cesse plus performantes, elles aussi.

Votre responsabilité

Il est sans doute inutile de redire que vous êtes responsables de vos données. Responsables devant votre équipe, vos patients et les autorités (Sécurité Sociale, Ordre, …). La durée de conservation évoluera sans doute dans les années à venir mais vous resterez redevables d'au moins 10 ans après la majorité de vos patients. Actuellement, cette donnée est, officiellement, à 30 ans pour le secteur libéral. C'était sûrement excessif lorsque vos caves regorgeaient de moulages. C'est peut être trop, l'auteur ne peut en juger, mais, aujourd'hui, 30 à 40 ans d'exercice tiennent dans la poche ! Pourquoi ne pas jouer le jeu ?

La goutte d'eau

Au fait, savez vous ce qui est le plus mal fait, aujourd'hui, concernant les sauvegardes ? Le test régulier. En effet, sauvegarder est essentiel, tout le monde le sait. Mais le jour où vous avez besoin de votre sauvegarde, si elle est vide ou plein de fichiers illisibles, que ferez-vous ? Alors, s'il vous plaît, testez (une fois par mois ?) une restauration. Le jour où vous en aurez vraiment besoin, vous serez efficace et pétri de confiance !

Conclusion

La multiplicité des risques liés à l'informatique devient telle que les mesures de sécurité doivent être toutes prises. Fiez vous à votre installateur, il est compétent et pourra vous proposer les bonnes solutions. Anti-virus, pare-feux, … les parades à chaque risque existent. Encore faut-il accepter de prendre conscience des besoins et de mettre en œuvre les solutions … adaptées à votre activité et non à celle de votre fournisseur ou de votre meilleur ami ! Et de leurs évolutions.

Votre profession a pu constater que les risques, entre autres les intrusions, existent. Puisqu'il est si difficile de se prémunir de tout, à vous d'en réduire les conséquences.. ■