FMH SERVICES

Cyberattaque, panne d’électricité, dégât d’eau : êtes-vous prêt à réagir ?

Que se passerait-il si vous ne pouviez soudain plus accéder aux données des patients de votre cabinet suite à une cyberattaque ? Ou si vos systèmes informatiques tombaient brusquement en panne ? Ce sont des questions désagréables. Il faut néanmoins se les poser.

Les entretiens avec les patients, la rédaction de rapports, la coordination des rendez-vous... Au quotidien, les professionnels de la santé ne trouvent guère le temps de répondre aux questions hypothétiques. Pourtant, des évènements imprévus peuvent se produire. Il peut par exemple s’agir de cyberattaques, de pannes de systèmes informatiques, d’une infiltration d’un terminal par un maliciel, de pannes d’électricité ou d’évènements naturels. Si l’on n’y est pas préparé, elles peuvent avoir de graves conséquences, paralyser le cabinet pendant des heures ou des jours, miner la confiance des patients ou avoir des conséquences juridiques avec des répercussions financières considérables. Cet article vous apporte des informations sur la manière dont vous pouvez vous préparer à une telle situation.

Élaborer un plan d’urgence
Imaginez que vous arrivez le matin dans votre cabinetet que les données de vos patients ne sont plus accessibles en raison d’une attaque par rançongiciel. Que faites-vous ? Vous appelez votre partenaire informatique ? Est-il préférable d’annuler les premières consultations des patients ? Quelles tâches votre assistante médicale assume-t-elle ? Pour ne pas devoir répondre à toutes ces questions dans le feu de l’action, c’est-à-dire dans un moment de stress et d’énervement, il vaut la peine d’avoir un plan d’urgence à disposition pour de telles situations exceptionnelles.

Vous pouvez procéder comme suit :
— Identifiez les menaces au moyen d’une analyse des risques que vous effectuez vous-même en toute bonne foi. Évaluez la probabilité et les dommages potentiels pouvant résulter de chacun de ces scénarios.
— Déterminez aussi les failles dans votre cabinet qui pourraient conduire à une urgence et remédiez-y vous-même ou avec l’aide d’un partenaire informatique externe.
— Développez, sur la base de votre analyse des risques, un plan d’urgence qui contient des instructions pour les scénarios éventuels. Vous pouvez catégoriser les différents scénarios qui ont des conséquences similaires et créer un plan d’action pour chaque catégorie. Important : définissez clairement les responsabilités de chaque collaborateur.
— Fixez également les règles de communication en situation de crise : comment et à quel moment informez-vous les membres de l’équipe, les patients, les prestataires informatiques et les partenaires ? À qui revient cette tâche ? Veuillez noter que les canaux de communication d’urgence ne doivent pas être les mêmes que ceux que vous utilisez dans votre travail quotidien, car ils pourraient également ne plus fonctionner. Il est également important d’avoir une liste de contacts à jour en permanence à disposition.

Former, vérifier et adapter
Plus vos collaborateurs sont à même de gérer des situations exceptionnelles, plus ils agiront avec assurance et efficacité en cas de crise. La formation de votre équipe aux situations d’urgence garantit le bon fonctionnement de votre plan d’urgence. La vérification du plan d’urgence à intervalles réguliers est également très importante : Répond-il encore aux exigences et risques actuels ? Faut-il l’adapter aux nouvelles technologies ou aux changements dans le cabinet ?

Sécuriser les données
Les cyberattaques poursuivent souvent le but de voler des données importantes pour l’entreprise. Les incidents tels qu’un dégât d’eau, un incendie dans la salle des serveurs ou la faillite du fournisseur de cloud peuvent également entraîner une perte totale ou partielle des données. Il est donc essentiel de sauvegarder les données afin d’être en mesure de récupérer les données importantes en cas d’incident. Instaurez des sauvegardes régulières. Pour cela, vous devez d’abord déterminer quelles données sont indispensables au fonctionnement de votre cabinet, par exemple les dossiers médicaux ou les données financières. Ces données sont prioritaires dans le plan de sauvegarde et devraient être sauvegardées quotidiennement. Pour les données de

moindre importance ou constantes, nous recommandons des cycles de sauvegarde hebdomadaires ou mensuels. Veillez à ce que vos données soient sauvegardées dans un endroit sûr, séparé des systèmes principaux et n'oubliez pas de tester régulièrement la récupération des données.

La règle 3-2-1 fait figure de référence pour la stratégie de sauvegarde :
— conserver 3 copies de toutes les données importantes (1 original et 2 sauvegardes) ;
— utiliser 2 supports de sauvegarde différents (p. ex. un disque dur externe et un espace cloud sécurisé) ;
— stocker 1 sauvegarde des données dans un endroit séparé du cabinet (p. ex. dans un coffre-fort privé).

Pour établir une sauvegarde des données fiable, il vaut la peine de faire appel à un spécialiste informatique.

Organiser le soutien externe
En cas d'urgence, vous n'avez pas le temps d'attendre... Veillez donc à ce qu'un soutien informatique externe soit disponible rapidement. Nous vous recommandons de conclure des accords de niveau de service (SLA) avec vos prestataires informatiques dans lesquels sont définis les prestations garanties et les temps de réaction.

Il vaut la peine de poser des questions désagréables
La préparation à d'éventuels scénarios de crise demande du temps et de la réflexion. Même si la plupart du temps, ces scénarios ne se produiront pas (espérons-le !) : le cas échéant, une préparation minutieuse apporte des réponses aux questions difficiles. Des réponses utiles qui contribuent à assurer le fonctionnement du cabinet et la sécurité des données sensibles des patients.

Partenaires informatiques externes : les points à observer
Le soutien par des prestataires informatiques externes est indispensable pour assurer le bon fonctionnement de l'infrastructure informatique et sa conformité avec les dispositions en matière de protection des données. Le partenaire choisi doit satisfaire aux exigences de la nouvelle loi sur la protection des données (nLPD) et garantir la sécurité et la protection des données des patients. Il doit donc...
— ... prouver qu'il respecte toutes les exigences en matière de protection des données, notamment en ce qui concerne la sécurité du traitement des données à caractère personnel. Vous le reconnaîtrez à ses certifications de sécurité, par exemple ISO/IEC 27001 (management de la sécurité de l'information) ou le label CyberSeal de l'Alliance Sécurité Digitale Suisse.
— ... présenter des mesures techniques et organisationnelles (TOM) documentées qui garantissent la sécurité du traitement des données, p. ex. l'utilisation du cryptage, les contrôles d'accès, les contrôles de sécurité réguliers.
— ... avoir de l'expérience dans le travail avec des données sensibles dans le domaine de la santé.
— ... accorder à votre cabinet le droit d'effectuer des audits et des contrôles réguliers.
— ... former régulièrement ses collaborateurs en matière de protection des données et de sécurité informatique.
— ... justifier de temps de réaction définis et d'une gestion des urgences documentée.
— ... être en mesure d'effectuer ou de soutenir une analyse d'impact relative à la protection des données personnelles (AIPD).

Vous devez conclure les accords suivants avec votre partenaire informatique :
— Accord de confidentialité (Non-Disclosure Agreement, NDA) : il garantit que tous les collaborateurs qui ont accès aux données des patients sont tenus au secret professionnel.
— Accord relatif à la sous-traitance : il régit la manière dont le prestataire informatique doit traiter et protéger les données.
— La FMH met à disposition des modèles pour les deux accords.

Daniel Huser
responsable du secteur gestion de projet & architecture IT

Health Info Net SA
Seidenstrasse 4
8304 Wallisellen
Tél. 0848 830 740
daniel.huser@hin.ch
www.hin.ch