Prendre en main la sécurité informatique du cabinet

Sécurité informatique Les objectifs nobles sont foison. Mais, pour certains d'entre eux, les bonnes intentions ne suffisent pas, il faut un plan solide. La sécurité informatique en fait partie. Nous vous montrons comment l'optimiser vous-même de manière progressive et pragmatique dans votre cabinet, en commençant par un inventaire informatique et un plan de sauvegarde.

Uwe Gempp, Philipp Senn

Une cyberattaque est un scénario menaçant l'existence même d'un cabinet médical. D'une part, des jours ou des semaines peuvent en effet s'écouler avant que tout fonctionne à nouveau normalement. Et d'autre, car la confiance des patients est durablement détériorée s'ils retrouvent leur dossier médical sur Internet. Qu'en est-il chez vous, êtes-vous paré pour un tel événement? En tant que médecin, propriétaire de cabinet, entrepreneuse, vous en remettez-vous à la chance ou y contribuez-vous avec système et planification?

En tant que médecin, vous êtes responsable des données sensibles de vos patientes et patients. Vous souhaitez améliorer la sécurité informatique de votre cabinet pour les protéger, mais ne savez pas par où commencer? La première étape du concept de protection [1] adapté à votre cabinet consiste à établir une vue d'ensemble. Vous posez les bases en établissant un inventaire informatique pertinent. Il pourra être utilisé directement pour le développement d'une stratégie de sauvegarde.

Assurer la transparence: tout commence par l'inventaire

L'un des plus grands défis pour la sécurité des données dans les cabinets médicaux est le manque de transparence de l'environnement informatique. Il est impossible de mettre en œuvre un concept de protection efficace sans avoir une vue d'ensemble des appareils, données et systèmes utilisés. La solution à ce problème réside dans un inventaire informatique exhaustif qui liste les ressources matérielles et logicielles du cabinet.

Pour l'inventaire informatique, tous les appareils sont d'abord répertoriés, en commençant par les ordinateurs, ainsi que les supports de données tels que les clés USB ou les disques durs externes, les appareils de laboratoire et autres appareils médicaux. Pour ce faire, vous pouvez utiliser notre modèle Excel [2] que vous trouverez à la fin de cet article. Pour chaque appareil, des informations telles que l'utilisation prévue, l'emplacement, les utilisateurs responsables, les données contenues et les versions de logiciels utilisées (système d'exploitation, antivirus, applications) sont consignées.

Les données de l'inventaire doivent être vérifiées et mises à jour au moins une fois par an [3]. Les nouveaux appareils sont immédiatement ajoutés à l'inventaire, ceux qui ne sont plus utilisés en sont retirés (ou la mention «hors service» ajoutée). Pour les appareils qui ont été mis hors service, il faut s'assurer que toutes les données ont été entièrement et définitivement supprimées avant de les jeter. Nous déconseillons de donner ou de vendre les appareils dont vous n'avez plus besoin [4].

Règle 3-2-1 de la sauvegarde

La règle 3-2-1 a fait ses preuves et est considérée comme la norme pour les stratégies de sauvegarde. Vous pouvez également l'appliquer à votre plan de sécurité:

- 3 copies de données (1 original et deux sauvegardes)
- 2 types de stockage différents (p. ex. un disque dure externe et une sauvegarde dans le cloud)
- 1 sauvegarde des données sur un site différent du cabinet (dans un coffre-fort privé, par exemple)

En appliquant la règle 3-2-1, vous augmentez la sécurité de vos sauvegardes. Les données restent intactes et accessibles même si un incendie détruit le cabinet ou si l'exploitant du cloud fait faillite. Cette règle n'a pas été inventée par un spécialiste en informatique, mais par un utilisateur concerné par une perte de données.

Rendre l'inventaire informatique utilisable: le plan de sécurité

Se charger d'un inventaire informatique pour lui-même n'est pas notre objectif. Nous souhaitons l'utiliser une première fois de manière productive – et développons une stratégie de sauvegarde. Il s'agit là d'un élément clé de notre concept de protection [5]. Elle garantit qu'en cas d'incident de sécurité – attaque par ransomware, incendie, dégât des eaux ou vol – les données importantes puissent être restaurées. En définissant quelles données et quels appareils doivent être sauvegardés, sur quel support de stockage et à quelle fréquence, le cabinet peut minimiser le risque de perte de données et contribuer à une reprise rapide des activités après l'incident.

Commencez par déterminer d'abord quelles données sont les plus importantes pour le fonctionnement du cabinet et doivent donc être prioritaires dans le plan de sauvegarde. Il peut s'agir de dossiers médicaux, de données financières et de toute autre information indispensable au fonctionnement quotidien du cabinet. Elles devraient être sécurisées chaque jour. Des cycles de sauvegarde hebdomadaires ou mensuels peuvent suffire pour les données moins importantes ou moins évolutives. Une fois cette question résolue, il est possible d'en déduire vos besoins de stockage et le calendrier approprié. Nous recommandons d'utiliser des disques durs externes pour la sauvegarde. Ces derniers devraient être conservés, si possible, en dehors du cabinet médical et bien fermés (voir encart). La sauvegarde dans le cloud est également possible, mais elle est soumise à des règles strictes liées à la loi sur la protection des données et de l'obligation de confidentialité professionnelle [6].

Une fois le plan de sauvegarde établi, il est temps de le mettre en œuvre. Des sauvegardes automatiques peuvent être mises en place à l'aide d'outils logiciels. En cas de doute, demandez l'aide d'un spécialiste. Testez ou faites tester régulièrement vos sauvegardes – au moins une fois par an. En effet, rien n'est plus inutile qu'une sauvegarde qui ne permet pas de restaurer les données en cas de problème.

Synthèse: inventaire informatique et stratégie de sauvegarde

- Établissez une liste de vos appareils en utilisant le modèle Excel – en commençant par vos ordinateurs.
- Saisissez les informations relatives aux appareils ainsi que les données enregistrées sur chaque appareil.
- Élaborez un plan de sécurité sur la base des informations de l'inventaire informatique. Ce dernier contient au moins une base de données, le support de stockage et les cycles de sauvegarde.
- Mettre en œuvre un plan de sauvegarde en configurant les supports de stockage et en mettant en place des sauvegardes automatiques.
- Une fois par an, restaurez les données de vos sauvegardes pour vous assurer qu'elles fonctionnent correctement.

Cet inventaire et la nouvelle stratégie de sauvegarde vous permettent non seulement de résoudre le problème fondamental de la transparence de votre environnement informatique, mais également de poser la première pierre d'un concept de protection informatique solide. En établissant un inventaire des équipements et des données et en utilisant ces informations pour mettre en œuvre un plan de sauvegarde, vous protégez votre cabinet contre les risques de perte de données et assurez la poursuite de son activité en cas de crise. D'autres instructions, check-lists et réponses aux questions fréquentes sur le thème de la sécurité informatique et utiles pour développer le concept de protection sont disponibles sur support.hin.ch.

© Kmitu / Dreamstime

Les éléments clés d'un concept de protection informatique sont l'inventaire et la sauvegarde

Correspondance
philipp.senn[at]hin.ch

Références
Liste complète des références sous www.bullmed.ch ou via code QR

Uwe Gempp
est Chief Security Officer (CSO) et architecte informatique chez Health Info Net SA (HIN).

Philipp Senn
est chef de projet Communication et intervenant en IT-Security / Awareness chez Health Info Net SA (HIN).