La sécurisation des données informatiques sensibles : "Un courrier électronique non chiffré n'est pas plus sûr qu'une carte postale"

Autor(en): **Loher, Marion**

Objekttyp: **Article**

Zeitschrift: **Curaviva : revue spécialisée**

Band (Jahr): **10 (2018)**

Heft 1: **Les médicaments : comment améliorer la sécurité de la médication en EMS?**

PDF erstellt am: **14.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-841450

La sécurisation des données informatiques sensibles

«Un courrier électronique non chiffré n'est pas plus sûr qu'une carte postale»

La digitalisation a permis de simplifier le traitement des données des patients: elles peuvent être sauvegardées, récupérées et transmises en quelques secondes. À l'ère de la cybercriminalité, il est important de pouvoir assurer un traitement sécurisé des données sensibles. Aussi en EMS.

Marion Loher

Et soudain… plus aucun accès aux dossiers informatisés des résidents! En novembre de l'année dernière, la maison de retraite régionale de Schöftland, en Argovie, a été la cible d'une cyberattaque. Après s'être introduits dans le système informatique de l'établissement, les hackers y ont installé un maliciel, bloquant tout accès aux dossiers des 108 résidentes et résidents. Dans la mesure où toutes ces données avaient été également sauvegardées sur support papier, le fonctionnement normal des services a pu être garanti. La sécurité ainsi que les processus de soins et d'accompagnement de l'ensemble des résidents ont ainsi été assurés, comme l'a confirmé à l'Aargauer Zeitung le directeur général de la maison de retraite, Thomas Seidle.

Les attaques de hackers contre des hôpitaux ou des centres de soins ne sont plus si rares. Dans la plupart des cas, elles provoquent la panne d'appareils médicaux ou verrouillent les données informatisées des patients, qui ne redeviennent accessibles que contre paiement d'une rançon. C'est ce qui s'est passé dans le cas de la maison de retraite de Schöftland. Comme rapporté dans divers médias, les maîtres-chanteurs avaient exigé un bitcoin pour déverrouiller les données bloquées – sachant qu'à l'époque des faits le bitcoin valait environ 7700 francs. L'institution a payé la somme exigée et les données bloquées ont été rendues à nouveau accessibles. La police n'a été informée qu'après-coup, ce qui n'a pas manqué de susciter des commentaires critiques de la part des services de police et des autorités. Comme l'explique Max Klaus, directeur adjoint de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI): «Nous déconseillons de payer une rançon. En premier lieu parce qu'il n'y a aucune garantie, dans le cas de chevaux de Troie informatiques, que la clé permettant de libérer les données bloquées soit effectivement envoyée en échange de la rançon. Ensuite parce qu'en payant, les victimes financent les pirates. Qui vont ensuite investir l'argent ainsi extorqué dans de nouveaux outils informatiques, d'où la certitude d'assister dans un avenir proche à de nouvelles attaques, encore plus sophistiquées.»

«N'importe quelle entreprise peut être la victime potentielle d'une cyberattaque.»

Des victimes choisies au hasard

L'expert fédéral ne considère pas que les établissements médico-sociaux constituent pour autant des cibles privilégiées pour des attaques de hackers: «N'importe quelle entreprise peut être la victime potentielle d'une cyberattaque», selon Max Klaus. «Beaucoup de ces attaques obéissent au 'principe de l'arrosoir'. Et leurs victimes sont la plupart du temps choisies de manière aléatoire.»

Tobias Fessler dirige l'unité informatique du Centre de soins régional de Baden. Il est du même avis: selon lui, les infrastructures médico-sociales destinées aux seniors ne sont pas plus particulièrement visées par les pirates informatiques que d'autres petites ou moyennes entreprises en Suisse. Mais il doit reconnaître que «son» propre centre de soins a déjà fait l'objet d'une attaque de ce genre. «Au printemps 2016, nous avons été la cible de plusieurs chevaux

de Troie informatiques en un laps de temps relativement court», explique-t-il. «Mais nos systèmes de pare-feu et nos mécanismes de sécurité ont extrêmement bien fonctionné. La défaillance du système n'a duré à chaque fois que quelques heures, un jour pour le cas le plus grave, et n'ont, pour chaque épisode, entraîné que quelques pertes de données sans conséquences: au pire deux ou trois documents Word ou Excel.» Ces attaques n'ont eu absolument aucun impact sur le quotidien ni sur les soins des résidents. «Nous n'avons même jamais envisagé d'entrer en matière sur le paiement d'une rançon.»

La Fondation de l'Âge d'or gère plusieurs établissements médico-sociaux pour personnes âgées dans la région de Genève. Jusqu'à présent, ils ont été épargnés par les cyberattaques, comme le confirme le directeur de la Fondation, Philippe Guéninchault, qui ajoute: «Par chance.» Car la Fondation de l'Âge d'or travaille également avec la saisie électronique des données. «Nous rassemblons toutes les données administratives et médicales utiles pour gérer au mieux les soins et les besoins de nos résidents. Ces informations sont indispensables pour organiser et coordonner les processus de soins de façon optimale mais également pour assurer le suivi en continu de toutes ces personnes.

Du pare-feu à la double identification

La saisie électronique des données est utilisée depuis 2011 par le Centre de soins de Baden. Ce qui signifie, selon Tobias Fessler, que «pratiquement tout» est enregistré et conservé. Toutes les informations concernant les résidents, pour commencer: «Cela va des détails et informations spécifiques sur la biographie de chacune et chacun de nos résidents, et de leurs préférences personnelles, en passant par les soins médicaux, la prise en charge et l'encadrement infirmier… et ce jusqu'à l'arrêt des prestations.» Ensuite, toutes les données concernant le personnel, y compris les données comptables. «Au quotidien, on peut dire qu'il n'y a pratiquement plus rien qui se fait sur support papier», relève le spécialiste en informatique.

Comment sécuriser des données digitales? «Chez nous, c'est le principe de bonnes pratiques qui prévaut», explique Tobias Fessler. «Nous avons mis sur pied un catalogue étendu de mesures, ainsi que des dispositifs de sécurité capables de s'activer lorsqu'ils détectent des schémas de comportement aléatoire dans le cadre de traitement de données, par exemple. Enfin, nous formons de manière continue et régulière toutes nos collaborateurs.» L'ensemble de l'infrastructure informatique de l'établissement est géré par une équipe de quatre spécialistes qui est en charge non seulement du Centre de soins régional de Baden mais également de la maison de retraite Kehl, soit un total d'environ 600 collaborateurs et 400 résidents.

Dans le cas de la Fondation genevoise de l'Âge d'or, les données sont hébergées par un prestataire informatique externe. «Ils garantissent l'intégrité de notre système et de nos données informatiques», explique le directeur Philippe Guéninchault. >>

De nombreuses données de résidents sont saisies électroniquement. Avec les bonnes mesures, elles peuvent être sécurisées Photo: Martin Glauser

PUBLIREPORTAGE

Les premiers foyers se raccordent au DEP

Une communication conforme aux principes de la protection des données est indispensable !

Les foyers et les institutions sociales sont obligés par la loi de transmettre et de recevoir les données personnelles sensibles de manière cryptée. HIN CURAVIVA Gateway permet de le faire simplement et en toute sécurité. Inscrivez-vous maintenant !

Quiconque envoie un e-mail avec des données sensibles de patient sans l'avoir crypté se rend punissable suivant les circonstances ! Car un e-mail non crypté peut être comparé à une carte postale : les informations relatives à l'expéditeur et au destinataire, ainsi que le contenu du message sont lisibles en clair et sont également transmis de cette manière sur Internet. Le courrier électronique non crypté comporte de grands dangers, car il ne garantit aucune confidentialité. Protégez-vous et protégez les données personnelles de vos résidents !

Grâce à Health Info Net AG (HIN), un standard aujourd'hui largement répandu a été créé en 1996 par le corps médical pour la communication sécurisée par e-mail. La plate-forme HIN rend l'échange d'informations électroniques simple et sûr dans le cadre de la collaboration interdisciplinaire. C'est pourquoi CURAVIVA a développé une offre commune avec HIN. Le HIN CURAVIVA Gateway : la solution associative à prix réduit – exclusivement pour vous en tant que membre CURAVIVA.

Le HIN CURAVIVA Gateway vous offre les avantages suivants :

- une communication sécurisée avec des e-mails conformes aux règles de la protection des données
- un accès sécurisé à diverses applications protégées par HIN
- une collaboration sécurisée dans l'espace membres protégé sur HIN Home

En outre, le HIN CURAVIVA Gateway vous offre toutes les conditions nécessaires pour participer au DEP : des identités électroniques et des moyens de communication conformes aux règles de la protection des données – lisez à ce propos l'interview d'Urs Kessler, de la fondation Amalie Widmer.

Voulez-vous, vous aussi, franchir le pas et vous moderniser – en terminer avec le fax et passer à l'e-mail et à eHealth ? Le HIN CURAVIVA Gateway rend l'échange de données électroniques simple, sûr et conforme aux règles de la protection des données. L'accès au dossier électronique du patient est, lui aussi, protégé par une identité HIN. **Découvrez-en plus : www.curaviva.ch/hin_fr**

La fondation Amalie Widmer, un centre de soin situé dans le canton de Zurich, a reconnu la modernité et l'importance de la protection et de lasécurisation des données. En tant que foyer de certification, ils se préparent au DEP comme des pionniers. Urs Kessler, chef de projet pour la documentation électronique des résidents, répond aux questions les plus importantes :

Monsieur Kessler, il semble que vous soyez le premier foyer en Suisse à être raccordé au dossier électronique du patient (DEP). Quelle aventure !
U. Kessler : C'est vraiment un beau défi d'établir et de mettre en œuvre quelque chose de nouveau avec différents acteurs. Dans notre travail quotidien, nous sommes en contact étroit avec divers prestataires de services. Grâce au DEP, nous pourrons échanger et rendre disponibles encore plus rapidement des données et des documents – c'est notre motivation ! Mais pour cela, il est important que tous se raccordent le plus rapidement possible au DEP. J'y vois à l'heure actuelle l'obstacle encore le plus important.

U. Kessler: «À la fondation Amalie Widmer, chaque professionnel de la santé recevra une identité électronique HIN pour accéder au DEP.»

Vous travaillez avec un HIN CURAVIVA Gateway. Où voyez-vous HIN dans le rôle de soutien sur le chemin du DEP ?
U. Kessler : HIN soutient le DEP par deux fonctions élémentaires : d'une part avec la communication conforme aux principes de la protection des données et, d'autre part, avec les conditions pour l'eID, qui sont mises en place grâce au HIN Access. L'eID permet d'accéder au domaine sécurisé du DEP, où sont enregistrés les documents qui sont pertinents pour le traitement. De cette manière, les processus de communication peuvent être créés plus efficacement, ce qui débouche sur une optimisation de la chaîne du traitement.
(Interview : Belinda Kreienbühl (Health Info Net AG)

Et pour ce qui est de la sécurité des données, le prestataire de services externe et l'institution en sont tous les deux conjointement responsables.

Le patient électronique

Pour Tobias Fessler, un archivage électronique des données des patients fait tout particulièrement sens. Il fait ici allusion au dossier électronique du patient (DEP). «La mise à disposition centralisée des données permet aux professionnels des soins infirmiers de disposer en tout temps de toutes les informations relatives à un résident particulier. Cela leur permet de travailler de manière plus efficace tout en renforçant la gestion de la qualité des soins». Philippe Guéninchault ajoute: «Le DEP nous permet d'échanger des informations entre les différents acteurs des diverses institutions impliquées, tout en gérant les autorisations d'accès réservées aux professionnels autorisés.»

«En l'absence d'une totale crédibilité, il sera très difficile au DEP de s'imposer.»

La loi fédérale sur le dossier électronique du patient est entrée en vigueur à mi-avril de l'an dernier. Elle oblige tous les hôpitaux et les établissements de soins à adopter le DEP après un délai transitoire de trois à cinq ans. Nicolai Lütschg est le directeur de la communauté de référence eHealth en Argovie, qui fonctionne comme centre de compétence pour la mise en place des dispositions de la loi fédérale sur le DEP dans le canton. Il est particulièrement conscient de l'importance d'assurer la sécurité et de garantir la protection des données. «En l'absence d'une totale crédibilité sur ce point, il sera très difficile au DEP de s'imposer concrètement.» C'est la raison pour laquelle toutes les institutions doivent faire partie d'une communauté de référence certifiée.

En ce qui concerne la protection des données, Nicolai Lütschg pense que le «double volontariat» des patients est également important: «Les patients doivent pouvoir décider s'ils souhaitent mettre en place un dossier digital. Et décider également de qui y a accès.» Il estime que le DEP aura une influence positive sur la qualité des soins prodigués et sur la sécurité du patient. En outre, il devrait renforcer l'efficacité du système de santé dans son ensemble, tout en développant les connaissances des patients et leurs compétences individuelles en la matière.

«Un bien précieux, qui doit être protégé»

En plus d'être sauvegardées et récupérées, les données concernant les patients doivent aussi pouvoir être transférées à un tiers en l'espace de quelques secondes. Lucas Schult, responsable informatique et directeur adjoint de Health Info Net SA (HIN), explique: «C'est bien pourquoi il est encore plus important que les règles concernant l'obligation de secret professionnel comme celles édictées par la loi sur la protection des données soient respectées. Cela implique en particulier le cryptage du courrier électronique.» La plateforme de Santé Electronique ou E-Health HIN met en réseau à travers toute la Suisse 22 000 professionnels de la santé et 750 institutions actives dans ce domaine (hôpitaux, laboratoires et établissements médico-sociaux). Selon Lucas Schult, l'élément central des services fournis par HIN ce sont «des identités digitales qui assurent un accès sécurisé, une communication sécurisée et un travail en collaboration sécurisé.» Des exigences de sécurité dont il explique qu'elles doivent s'appliquer, par exemple, au DEP. Les membres de Curaviva Suisse bénéficient de cette offre depuis juillet 2017, via le raccordement HIN Curaviva.

Lucas Schult compare un courrier électronique non crypté avec une carte postale: «Les informations concernant l'expéditeur et celles concernant le destinataire, tout comme le contenu même du message, apparaissent en clair. Ces informations voyagent également en clair sur le Net. Tout le monde peut les lire. Tout au long de son parcours, un courrier électronique peut être intercepté: n'importe où et à n'importe quel moment. Et être automatiquement analysé et manipulé. Aucun message envoyé sur le Net n'est sans danger, certains considérables, et les courriers électroniques ne sont absolument pas confidentiels.» C'est précisément la raison pour laquelle il est si important de crypter les messages électroniques. Pour le responsable informatique de HIN: «Les données personnelles de façon générale, et les données médicales en particulier, sont un bien précieux et doivent être protégées». Faire changer les choses dans ce domaine, voilà, pour Lucas Schult, l'un des plus grands défis des années à venir. «Nous devons former les collaborateurs de façon plus spécifique encore sur la sécurité informatique. Et utiliser de manière plus systématique les possibilités techniques dont nous disposons pour protéger les données médicales sensibles de la cybercriminalité».

Un manque de connaissances et de moyens

Tobias Fessler, du Centre de soins régional de Baden, estime qu'il reste encore beaucoup à faire dans ce domaine. «Avant tout dans les petites institutions, où le domaine informatique a été négligé de façon inexcusable, ce qui, en ces temps de cybermenaces croissantes est absolument catastrophique et peut se révéler fatal». D'après lui, l'éducation et la formation continue des collaborateurs en matière d'informatique et de cybersécurité permettraient déjà d'aider à contrer efficacement ces menaces. Par ailleurs, il estime qu'il serait extrêmement utile de dresser une liste de toutes les questions relatives à la sécurité des données et à leur protection, pour en faire une sorte de document de référence et de code de bonnes pratiques à l'usage de tous les EMS.

Max Klaus, de la Centrale MELANI, partage son analyse: «Les PME aujourd'hui manquent souvent des compétences et des moyens financiers nécessaires pour mettre sur pied un département informatique suffisamment sécurisé. On observe ce manque dans toutes les branches d'activité, pas seulement en ce qui concerne les établissements médico-sociaux.» Le conseil de l'expert au cas où des hackers frapperaient, comme dans le cas de la maison de retraite de Schöftland: «Ne pas céder au chantage. Appeler Immédiatement la police. Et déposer plainte.» ●

Texte traduit de l'allemand