Les établissements de soins ne sont pas à l'abri de la cybercriminalité : les données des patients sont des "otages" lucratifs

Autor(en): **Weiss, Claudia**

Objekttyp: **Article**

Zeitschrift: **Curaviva : revue spécialisée**

Band (Jahr): **8 (2016)**

Heft 3: **Communication : les EMS entrent dans l'ère 2.0**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-813798

Les établissements de soins ne sont pas à l'abri de la cybercriminalité

Les données des patients sont des «otages» lucratifs

L'échange rapide et efficace des données médicales présente de gros avantages. Et des dangers aussi: s'ils facilitent la communication entre les institutions, les dossiers électroniques des patients sont aussi exposés aux cyberattaques. Des experts expliquent quelles sont les menaces qui guettent et comment les gérer.

Claudia Weiss

Paralysie des ordinateurs du bloc opératoire, systèmes d'infusion qui déraillent ou dossiers électroniques de patients pris en otage pour exiger le paiement d'une rançon: ce qui ressemble à un film de science-fiction est pourtant déjà la réalité aujourd'hui. De tels scénarios vont encore donner bien du fil à retordre aux experts en sécurité au cours des années à venir: la stratégie de la Confédération, qui vise à mettre en réseau l'ensemble des dossiers électroniques des patients et à y permettre aussi l'accès depuis l'étranger en cas d'urgence, est séduisante et doit être réalisée aussi vite que possible, selon le Conseil fédéral. Avant cela, cependant, la sécurité de toutes les données sensibles des patients doit être garantie.

L'organe de coordination Confédération-cantons, eHealth Suisse, se veut rassurant et estime que la menace n'est pas très grande: «Aujourd' hui déjà, de nombreuses données sont enregistrées sous forme électronique», peut-on lire dans un document en ligne sur le thème de la sécurité. «Elles ont beau avoir un caractère hautement personnel, elles ne constituent pas, comme les données bancaires, une source d'enrichissement. Elles n'offrent donc qu'un intérêt limité pour les cyberpirates.» Cela paraît convaincant. Et rassurant. S'il n'y avait des rapports contradictoires.

Panda Security, par exemple, un fournisseur de logiciels et de solutions de sécurité, a récemment publié un dossier complet sur le thème «The Cyber Pandemic», qui brosse une autre réalité: selon ce rapport, les hôpitaux, les cliniques et les laboratoires sont justement «de plus en plus souvent la cible de cyberpirates». En 2015, 253 failles de sécurité seraient apparues dans le secteur de la santé, plus de 500 personnes auraient été concernées et 112 millions de données volées. «Les données médicales sont très précieuses et hautement sensibles, et qui que ce soit qui contrôle ces données peut en tirer d'énormes profits», ainsi qu'il est écrit dans le dossier. Cela contredit le point de vue de eHealth Suisse. Qu'en est-il alors: les données de santé sont-elles menacées ou non?

Menaces croissantes sur le secteur de la santé

Les experts apportent une réponse peu engageante: au cours de ces dernières années, les hôpitaux ont été attaqués avec plus de force que ne l'ont été d'autres branches. Martin Leuthold, responsable de la division sécurité de la Fondation Switch, affirme: «Le secteur de la santé enregistre la deuxième plus forte croissance en terme d'incidents.» Selon les derniers rapports en date, le secteur de la santé est la principale cible des attaques, après les organisations gouvernementales, mais avant les banques et l'industrie. Peter E. Fischer, responsable du centre de compétence Sécurité de l'information & Protection des données dans le domaine de la santé de la Haute Ecole spécialisée de Lucerne et président de la Swiss Internet Security Alliance (SISA), voit un danger croissant: «Selon le dernier IBM Cyber Security Intelligence Index, les menaces ont augmenté de près de deux tiers en 2015 par rapport à 2014.»

Il confirme, certes, ce qu'affirme eHealth Suisse, à savoir qu'un vol de données de santé ou une manipulation d'appareils médicaux ne procure pas un enrichissement direct. Pourtant: «Les données et les appareils sont si sensibles que le dommage peut être bien plus élevé qu'un retrait d'argent non autorisé sur un compte.» La publication d'un dossier médical peut avoir pour

La saisie électronique des données du patient facilite l'échange entre unités et même entre institutions. Mais tout ce qui est en réseau mérite une protection particulière. Photo: Martin Glauser

conséquence que la personne ne trouve plus d'emploi ou qu'elle est mise au ban de la société. Des répercussions importantes, donc, qui pourraient aussi très bien pousser les personnes concernées à verser beaucoup d'argent pour récupérer leurs données. Ces derniers temps, les prises en otage de données avec des «ransomware» sont devenues les menaces les plus courantes et les plus dangereuses. «Le système de santé suisse serait bien inspiré de ne pas prendre à la légère la valeur des données de santé ni les dangers qui les menacent», avertit Martin Leuthold de Switch.

Et eHealth Suisse est bien conscient des risques: «Il ne fait aucun doute que les menaces et la sécurité des données ont gagné en importance ces dernières années», confirme Adrian Schmid, responsable du secrétariat. A ce jour, toutefois, le système de santé suisse ne connaît pratiquement aucun cas concret de vol de données électroniques. Dans la plupart des exemples de notoriété publique, ce sont des personnes qui détenaient des droits d'accès qui auraient volé les informations – ce fut notamment le cas concernant la publication du dossier médical du pilote de Formule 1 Michael Schumacher. «Dans le quotidien, les actes malveillants des personnes autorisées posent certainement davantage de problèmes que les attaques techniques provenant de l'extérieur», affirme Adrian Schmid. Avant d'ajouter: «Le projet sur les dispositions d'exécution de la Confédération pour le dossier électronique du patient comporte beaucoup de dispositions concernant la sécurité des données.» Ce projet précise dans le détail qui est responsable de quoi en matière de protection et de sécurité des données. Par exemple au point 4.15.1: «Les communautés doivent veiller à la protection et à la sécurité des données tout au long du cycle de vie des systèmes du dossier électronique du patient. A cet effet, il est nécessaire de définir, d'introduire et de respecter des processus formels de documentation, de spécification, de test, de contrôle qualité et de mise en œuvre contrôlée pour: l'introduction ou le développement de nouveaux systèmes [4.15.1.1]; les modifications ou développements majeurs réalisés sur les systèmes existants [4.15.1.2]; le changement des plateformes d'exploitation [4.15.1.3].» Ces indications si précises déterminent ainsi un standard qui permettrait aussi, selon Adrian Schmid, de sécuriser l'échange de données de santé hors du dossier électronique du patient.

Les prises en otage des données sont les menaces les plus courantes et les plus dangereuses.

Les attaques contre les hôpitaux se multiplient

Mais les exigences élevées vont encore mettre à contribution les responsables informatiques des structures dans le domaine de la santé. Car les cas que Panda Security a recensés aux Etats-Unis ne sont pas anodins: «Hôpitaux et cliniques universitaires de Utah: les données de 2,2 millions de patients ont été volées.» «Compagnie d'assurance Anthem: accès à 80 millions de dossiers de clients.» «Centre presbytérien de médecine à Hollywood: rançon de 3,7 millions de dollars exigée.» Panda Security parle avant tout d'attaques «ransomware», avec un logiciel qui s'empare des données et qu'on ne peut récupérer que contre le versement d'une rançon. L'Allemagne aussi a déjà connu des cas de cyberracket, par exemple l'hôpital Lukas, à Neuss, et les établissements hospitaliers Klinikum, à Arnsberg.

En Suisse, les hôpitaux ne seraient pas à l'abri non plus, dit-on à la division sécurité de la Fondation Switch: «A notre avis, les organisations du domaine de la santé en Suisse doivent aussi s'attendre à être plus souvent attaquées», avertit l'expert en sécurité Martin Leuthold. Et Peter Fischer de la Haute école spécialisée de Lucerne d'ajouter: «Nous avons eu connaissance de tentatives de hacking dans les hôpitaux suisses aussi. Les >>

exemples montrent que les établissements de santé sont particulièrement menacés et qu'ils doivent par conséquent être encore beaucoup mieux protégés.» Selon lui, divers dangers menacent: un blocage total des données ou une revente des données sont tout autant possibles qu'une demande de rançon pour récupérer les données ou des attaques d'instruments pilotés électroniquement comme des pompes à insuline, des moniteurs de surveillance ou des stimulateurs cardiaques. «Ce sont tous des dangers potentiels réels», résume-t-il.

Peter Fischer explique aussi pourquoi le système de santé est de plus en plus vulnérable face aux attaques des hackers: «Bien sûr, de nombreux médecins et hôpitaux font aujourd'hui déjà des saisies électroniques des multiples données des patients.» Seulement «ces données sont le plus souvent enregistrées localement, c'est-à-dire sur le serveur de l'hôpital.» Le dossier électronique du patient, en revanche, qui serait sauvegardé sur le cloud et qui pourrait être consulté depuis n'importe où par les personnes autorisées, offre bien davantage de prise aux attaques. A cela s'ajoute le fait que la technique de l'information n'est pas une compétence clé du système de santé, «et encore moins la sécurité de l'information».

L'homme représente le plus grand risque

Chez Switch, les professionnels de la sécurité savent aussi exactement où se situe le problème: la technologie médicale est de plus en plus connectée à l'interne, mais du point de vue de la sécurité, elle n'est pas armée pour affronter les menaces qui règnent sur Internet. «D'abord parce que les systèmes médicaux sont conçus pour une durée de vie bien plus longue. A l'origine, ils n'ont pas été développés pour un monde connecté et par conséquent exposé à des dangers. Après quelques années, il devient difficile de protéger ces systèmes contre des menaces qui évoluent sans cesse très vite», explique Martin Leuthold. En outre, les hôpitaux gèrent des systèmes d'information très complexes, et ils traitent et enregistrent un volume très important de données. Et si ce n'est pas le système lui-même qui est en cause, reste alors toujours l'accès au plus grand point faible du système: l'homme, qui ouvre sans le vouloir un e-mail de «phishing» (hameçonnage) et qui donne ainsi accès au système. L'homme représente donc le plus grand risque. D'un côté, ce n'est pas très bon, car l'erreur restera toujours humaine. De l'autre, cela signifie aussi que les organisations ne restent pas impuissantes face aux cyberattaques, car l'homme est capable d'apprendre. «Cela nécessite avant tout une prise de conscience et une intervention adéquate de toutes les personnes qui ont à faire avec ces données et ces appareils. C'est là qu'il y a la plus grande faille, donc le plus grand danger, et c'est là par conséquent qu'il est le plus urgent d'agir», explique Peter Fischer de la Haute école spécialisée de Lucerne.

Switch a résumé les principales recommandations en matière de gestion de la sécurité sur Internet (lire l'encadré). Les hôpitaux seraient conscients de leur responsabilité, avance Martin Leuthold, ils maîtrisent les systèmes de gestion de la sécurité de l'information et de la sécurité informatique conformément aux «bonnes pratiques» actuelles. «Seulement, le crime organisé sur internet (la cybercriminalité) évolue si vite que ces mesures ne suffisent plus à elles seules aujourd'hui, et la défense doit être renforcée. Pour cela, notamment, la capacité à identifier rapidement les attaques perpétrées est un point essentiel, de même que la capacité à lutter rapidement contre les attaques identifiées. «Chez Switch, nous nous concentrons depuis des années sur ces thèmes», explique l'expert en sécurité. «Mais il n'y a pas de possibilités techniques pour supprimer les failles techniques existantes, d'autant moins dans la technologie médicale qui intègre souvent des systèmes dépassés et dont la mise à jour est généralement très fastidieuse en raison des normes juridiques.» Pour pouvoir malgré tout concevoir une protection parfaitement sûre, les hôpitaux ne peuvent pas travailler chacun seul dans son coin, mais doivent pouvoir s'appuyer sur un «regroupement des moyens dans des centres de compétences communs».

Des domaines bien protégés

Une consolation: «Les deux domaines de premier niveau à extension .ch et .li gérés par Switch sont reconnus comme les

Les dangers qui guettent sur Internet

Switch a produit un résumé des délits les plus courants sur Internet et des mesures à prendre pour s'en protéger (www.switch.ch).

Ransomware:

De plus en plus souvent, les cybercriminels bloquent l'accès aux données et exigent une rançon pour les libérer. Les attaquants ont même installé pour cela leurs propres helpdesks qui renseignent les intéressés.

Chantage par attaques DDoS:

Des groupes menacent de paralyser des services en ligne en inondant un réseau par des masses de demandes (Distributed Denial of Service, attaques par déni de service, abrégées attaques DDoS) si l'on ne paie pas. L'expérience montre que payer ne sert à rien, au contraire: ils ne sont qu'un signal pour plus d'argent, sans quoi l'obstruction d'accès augmente. En cas de menace, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani) recommande d'avertir la police et de prendre les mesures techniques de sécurité pour contrer l'attaque.

APT (Advanced Persistant Threat) avec de nouvelles dimensions:

Les auteurs espionnent leurs victimes durant un temps prolongé avant de lancer des attaques sur mesure. Si, par le passé, les motivations relevaient davantage des services secrets, elles sont aujourd'hui de nature monétaire. C'est du moins la conclusion que l'on peut tirer du cas Carbanak, du nom du logiciel malicieux mis en œuvre par un groupe criminel qui a attendu deux ans avant d'attaquer. Il a piraté les comptes utilisateurs de banques, a pris le contrôle des caméras de surveillance et a programmé les distributeurs automatiques de billets de façon à ce qu'ils délivrent des billets d'une valeur plus élevée que celle enregistrée par le logiciel. Le dommage s'est monté à près d'un milliard de dollars US et à touché une centaine de banques dans trente pays.

Conseils pour contrer les cyberattaques

Backup
Faites régulièrement un backup des données de votre ordinateur, par exemple sur un disque dur externe ou sur le cloud.
Scanner antivirus
Installez un programme de protection antivirus – de préférence avec une mise à jour automatique de la liste des virus.
Pare-feu
Installez un pare-feu. Il vous avertit en cas de problèmes sur Internet.
Mises à jour
Téléchargez régulièrement les mises à jour pour vos programmes, plug-ins et applications et installez toujours les versions les plus récentes. Elles comportent des patches pour les points vulnérables connus.
Mots de passe
Modifiez souvent les mots de passe de vos comptes bancaires, de vos comptes e-mail ainsi que de tous les services que vous utilisez en ligne. Utilisez une suite de lettres, chiffres et signes difficile à craquer. Ne notez nulle part vos mots de passe par écrit, mais utilisez-en qui soient faciles à mémoriser.
Prudence
Soyez prudent avec la transmission ou l'enregistrement de vos données. Ne cliquez pas non plus sur chaque lien dans les e-mails ou dans les actualités Facebook. Demandez-vous d'abord s'il peut s'agir d'un leurre. C'est aussi valable pour l'ouverture des fichiers joints dans les e-mails. Par le passé, les e-mails frauduleux de hameçonnage comportaient des fautes ou des signes erronés. Depuis, les textes s'améliorent sans cesse et sont de plus en plus crédibles. Les cybercriminels utilisent également des annonces dans la presse pour disséminer leurs mails frauduleux.
Contrôle de sécurité SISA
Une fois par mois, faites un contrôle de sécurité SISA (Swiss Internet Security Alliance, www.swiss-isa.ch)
Adblocker
Installez un Adblocker

plus sûrs du genre au monde», assure Martin Leuthold. «C'est le résultat d'une étroite collaboration entre l'Office fédéral pour la communication, Switch en tant que fournisseur d'accès, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani) et le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI).» Cette collaboration permettrait de désactiver dans les 24 heures des domaines utilisés frauduleusement pour des e-mails de hameçonnage et des logiciels malveillants (malware), si le détenteur du domaine ne règle pas le problème. «De cette façon, il est moins intéressant pour les cybercriminels d'utiliser frauduleusement les domaines à extension .ch et .li, et les domaines qui ont été la cible d'attaques sont plus rapidement nettoyés ou fermés.»

«La sécurité absolue n'a jamais existé et n'existera jamais nulle part.»

Face à de tels dangers, la question se pose tout de même de savoir si un échange électronique de données de patients est vraiment judicieux. Pour les experts, cette question ne se pose même pas: «Le retour aux dossiers papier, comme le préconisent quelques hôpitaux aux Etats-Unis, ne peut pas être la bonne option», affirme Peter Fischer. «Pour les fournisseurs de prestations, disposer de données électroniques présente des avantages évidents et indispensables.» Sans accès aux données des patients, insiste-t-il, nous aurions aujourd'hui déjà des problèmes récurrents: des examens inutilement prescrits à double, des patients qui donnent de mémoire des informations erronées et les ruptures de transmission, c'est-à-dire les erreurs qui surviennent au moment de la transmission sur un autre support, par exemple du papier à l'e-mail ou inversement. L'identification des signaux d'alarme serait ainsi aussi laissée au hasard, lorsque les appareils médicaux ne sont pas connectés et ne peuvent pas, de ce fait, être surveillés à distance. «Avec la pénurie actuelle de personnel, il n'est d'ailleurs pas pensable de surveiller les appareils sur place, sans même parler de l'aspect économique», souligne encore Peter Fischer. «La question n'est donc pas de savoir si nous recourons ou non à la solution électronique, mais comment.»

«On ne peut pas atteindre cent pour cent de sécurité», reconnaît aussi Martin Leuthold de Switch. «Mais il suffit que les organisations élèvent leur sécurité à un niveau tel que les cyberpirates ‹fainéants› préfèrent aller attaquer des organisations moins bien sécurisées.» Selon Peter Fischer, le tour de force est de pouvoir associer «la meilleure sécurité possible, une bonne praticabilité et la compatibilité économique». Mais il est lui aussi réaliste: une sécurité absolue n'existe pas dans la e-technologie. «Elle n'a jamais existé nulle part et n'existera non plus nulle part. C'est valable pour la sécurité de l'information, mais c'est aussi valable pour la circulation routière», dit-il. Et pourtant personne ne se demande s'il faudrait renoncer à la circulation routière. Outre les conditions technologiques, les composantes humaines de «prise de conscience» et de «compétences opérationnelles» sont nécessaires, tant pour la circulation routière que pour le dossier électronique du patient.

L'objectif est de diminuer le plus possible le risque résiduel, de façon à ce que les divers avantages l'emportent incontestablement. «C'est pourquoi il importe que toutes les parties prenantes comme les médecins, les soignants, les prestataires de solutions et aussi les hautes écoles collaborent étroitement afin de développer une bonne solution et de gagner ainsi la confiance des patientes et des patients.» Alors seulement de nombreux patients se décideront à ouvrir un dossier électronique du patient. Et ainsi seulement eHealth Suisse réussira ce que le Conseil fédéral s'est donné pour objectif: «Garantir à la population suisse l'accès à un système de santé de qualité, efficient, sûr et avantageux financièrement.» ●