# Protection et sécurité des données informatiques : "La menace de la cybercriminalité a considérablement augmenté"

Autor(en): **Seifert, Elisabeth**

Objekttyp: **Article**

Zeitschrift: **Curaviva : revue spécialisée**

Band (Jahr): **11 (2019)**

Heft 2: **Numérisation : quels défis et quelles chances pour les institutions?**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-885936

**Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

**Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

**http://www.e-periodica.ch**

## Protection et sécurité des données informatiques

# «La menace de la cybercriminalité a considérablement augmenté»

**Les institutions du domaine de la santé et du social ne se préoccupent généralement pas assez de la sécurité des données. Il ne suffit plus aujourd'hui de disposer d'un bon ordinateur. La cybercriminalité croissante et la multiplication des connexions digitales obligent à des mesures plus drastiques.**

Elisabeth Seifert

Même une infrastructure informatique techniquement à jour n'est pas à l'abri des virus (chevaux de Troie et autres maliciels), comme l'a découvert André Rotzetter, conseiller en cybersanté pour des établissement de soins et directeur de l'association Altersbetreuung im oberen Fricktal, dans le canton d'Argovie, qui regroupe deux institutions avec 200 résidents au total. Malgré un pare-feu et un programme anti-virus sophistiqués, son système informatique a été contaminé. En effet, la plus performante des protections ne peut identifier qu'un virus déjà connu.

L'intrus (encore) inconnu était installé dans un document PDF envoyé par un candidat. À peine André Rotzetter avait-il ouvert la pièce jointe que le système a planté. Seule option possible: «Pour limiter les dégâts, nous avons immédiatement déconnecté tous les ordinateurs du Net». Ce qui a effectivement permis de limiter le dommage. Car ce cas de figure avait été prévu: une sauvegarde interne quotidienne de toutes les données et transactions, est effectuée à midi et transférée chaque soir sur le serveur externe et hautement sécurisé d'une entreprise spécialisée, pour limiter les pertes en cas d'attaque, et, au pire des cas, ne perdre que l'équivalent d'une demi-journée de travail.

**«Les entreprises insuffisamment protégées sont prises dans les mailles du filet.»**

Le centre pour personnes âgées de Schöftland, en Argovie, était, lui, nettement moins bien préparé pour faire face à ce genre de piratage informatique. Ce qui lui a valu de se retrouver en une des journaux en décembre 2017, lorsqu'un virus a bloqué en quelques secondes les données d'une centaine de ses résidents, les rendant totalement inaccessibles. L'institution n'a pu les récupérer qu'une fois payée la rançon réclamée par les cyberpirates.

### La digitalisation sensibilise à la protection des données

Ces deux cyberattaques ne sont pas des cas isolés. Nombreuses sont les entreprises suisses, y compris celles actives dans les domaines de la santé et du social, qui ont déjà eu à faire face au moins une fois à ce type d'agression. «La menace de la cybercriminalité a considérablement augmenté», selon Lukas Fässler, avocat spécialisé dans la protection des données et la sécurité informatique. Les institutions sociales et celles du secteur de la santé sont particulièrement concernées, pour deux raisons: d'une part parce que la vente de données de patients piratées rapporte beaucoup d'argent, d'autre part parce que – c'était le cas de Schöftland – elles sont extrêmement vulnérables au chantage en cas de bug causé par des virus.

Être piraté même lorsqu'on est une PME active dans le social ou la santé, c'est un danger bien réel, comme le souligne Philine Richert, Chief Information Security Officer chez Swisscom Health, une filiale de Swisscom spécialisée dans les solutions informatiques dans le domaine de la santé. La plupart du temps, ce type d'attaque ne cible pas une institution en particulier – il s'agit plutôt d'attaques de masse, opérées par les pirates pour tenter d'infiltrer le plus grand nombre possible de systèmes. «C'est

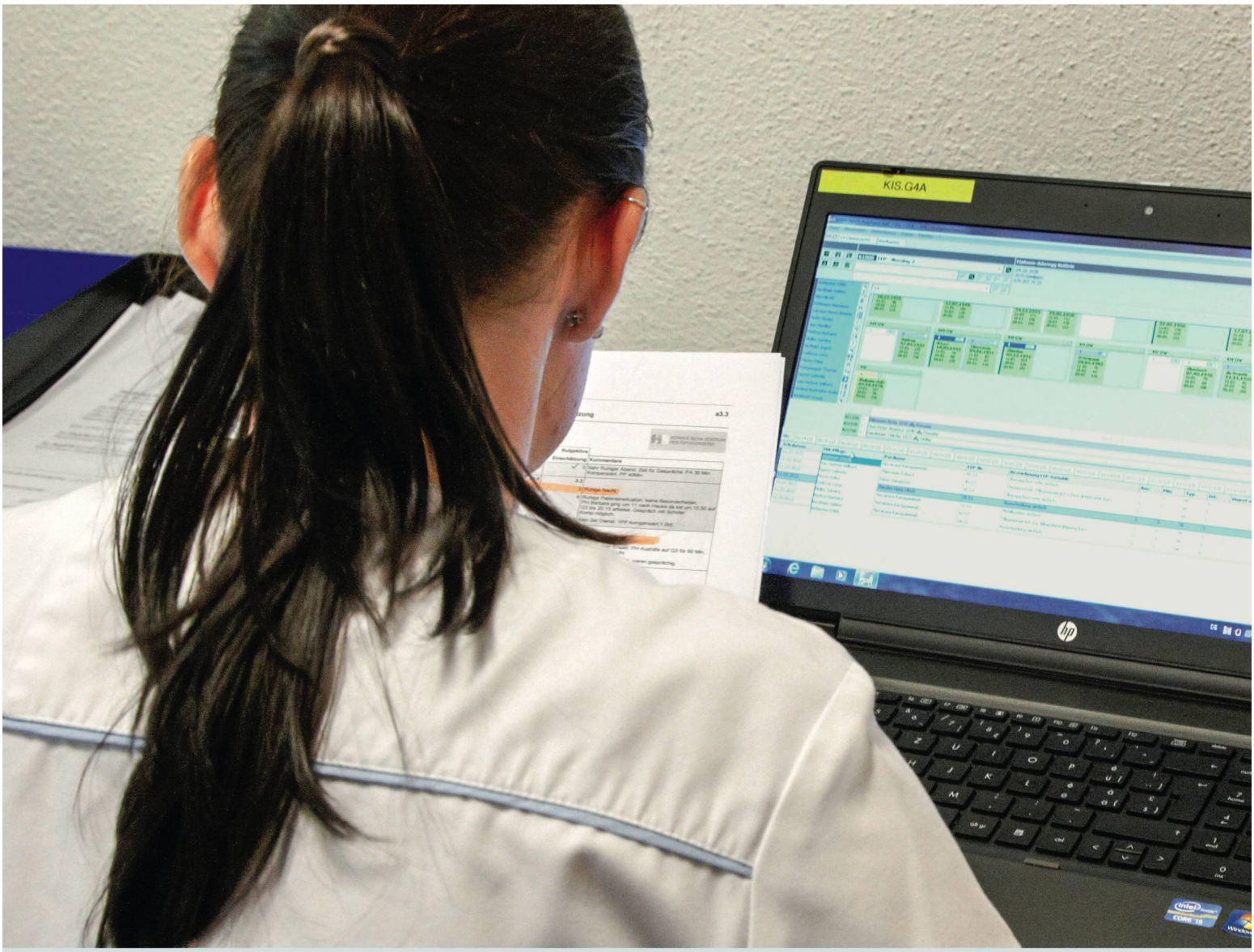
comme la pêche au chalut: les entreprises insuffisamment protégées ont prises dans les mailles du filet». Une attaque réussie est souvent suivie d'une demande de rançon, notamment pour pouvoir récupérer les données piratées.

**Des données personnelles sensibles**

Pour les entreprises touchées, les conséquences dépassent depuis longtemps le seul impact financier. Comme le précise Philine Richer, des cliniques et des hôpitaux ont parfois été obligés de différer traitements et opérations. Dans des établissements médico-sociaux, les plannings de soins et de médication informatisés ne sont soudain plus accessibles. Outre le fait que des cyberattaques peuvent impacter la prise en charge comme le processus de soins, le secteur social comme celui de la santé travaillent toujours avec des données personnelles sensibles. Lorsque ce type de données est piraté ou volé, les dégâts d'image pour les institutions concernées sont considérables. Avec l'informatisation croissante de tout ce qui relève de l'administratif, mais aussi des soins, la protection des données et la sécurité informatique prennent de plus en plus d'importance.

**«La loi sur la protection des données reste un gaspillage de papier.»**

Les défis auxquels doit faire face notre société numérisée dans ces deux domaines se traduisent également en termes de réglementation. L'an dernier, diverses dispositions destinées à renforcer le droit existant sont entrées en vigueur au sein de l'UE. Comme le souligne Lukas Fässler, ces dispositions devraient être intégrées dans la révision totale de la loi fédérale sur la protection des données actuellement en cours. Dans l'espace européen, les entreprises doivent pouvoir prouver, documents à l'appui, qu'elles respectent cette réglementation. Pour ce faire, elles sont tenues de désigner un ou une responsable, en charge d'inventorier l'ensemble des données sensibles, >>




Les mesures de sécurité ne sont utiles que si les collaborateurs sont sensibilisés aux questions de sécurité. Photo: Martin Glauser

## Le dossier électronique du patient est-il sûr?

Dès le mois d'avril 2022, tous les établissements médico-sociaux et institutions pour personnes en situation de handicap décomptant à charge de l'assurance obligatoire des soins, devront proposer un dossier électronique du patient (DEP) à leurs résidentes et résidents qui le souhaitent. Le délai pour les hôpitaux est fixé au mois d'avril 2020 déjà.

Les informations accessibles dans le DEP demeurent en principe dans le système d'information primaire du prestataire, c'est-à-dire des EMS, des hôpitaux ou encore des médecins de famille. Le DEP ne stocke aucune donnée. Il renvoie simplement aux lieux de stockage des données, il récupère et édite les données au moment de la requête. Cette mise en réseau passe par une plateforme eHealth. En Suisse, Swisscom et La Poste sont les deux principaux opérateurs de plateformes. Les différents prestataires sont connectés à une plateforme eHealth par le biais de leur affiliation à une communauté ou une communauté de référence chargée d'assurer les conditions techniques et organisationnelles.

Tandis que le contact avec les prestataires et les patients est principalement de la responsabilité des communautés de référence, les opérateurs de plateformes interviennent au titre de fournisseurs techniques, garants du bon fonctionnement et de la gestion des pannes de la plateforme eHealth et du DEP. Comme l'écrit La Poste suite à une demande de la Revue spécialisée, elle garantit aux communautés de référence la certification du DEP. Les communautés de référence – et donc indirectement aussi les opérateurs de plateformes – seront mis à l'épreuve dans les mois à venir à la demande de la Confédération. Les questions liées à la sécurité seront alors minutieusement examinées. Aussi bien Swisscom que La Poste s'engagent à respecter les mesures de sécurité les plus strictes. La mise en réseau des informations se déroule dans des centres de données les plus modernes de Suisse.

Les mesures de sécurité portent notamment sur l'identité électronique dont les patients et les professionnels de la santé ont besoin pour utiliser le DEP. Cette identité électronique peut être obtenue auprès des éditeurs de moyens d'identification. Pour avoir accès au DEP, les éditeurs de moyens d'identification doivent être certifiés par la Confédération. Une autre mesure de sécurité prescrite par la loi exige un mot de passe fort avec double authentification. Par ailleurs, les patients décident librement à quelles institutions et professionnels de la santé ils accordent les droits d'accès à leur DEP et pour quelle durée. Les cas d'urgence médicale font exception, la loi autorisant les professionnels de la santé d'accéder aux données du dossier même sans droits d'accès.

Malgré toutes les mesures de sécurité, des actes malveillants envers le dispositif informatique ne peuvent jamais être totalement exclus, affirme-t-on encore du côté de La Poste. Dans le cas du DEP, les auteurs devraient d'abord pirater l'identité électronique d'un patient puis contourner ensuite la double authentification.

en précisant où et comment elles sont enregistrées, et qui sont les personnes habilitées à les traiter. S'ajoute à cela l'obligation de procéder à une analyse des risques et de prendre les mesures nécessaires pour les minimiser et éviter qu'elles ne tombent entre de mauvaises mains. «L'obligation d'inventorier les données sensibles est en fait déjà entrée en vigueur, mais elle reste lettre morte», déplore-t-il. «La loi sur la protection des données reste un gaspillage de papier».

**Envoyer des données de patients par e-mail non sécurisé est punissable.**

**«Les institutions s'y mettent… lentement»**

Dans un contexte où la cybercriminalité ne cesse d'augmenter, observe Lukas Fässler, le grand public est de plus en plus sensibilisé à ces questions. Pour les établissements médico-sociaux, cet intérêt croissant va de pair avec l'introduction obligatoire d'ici 2022 du dossier électronique du patient. La mise en réseau des établissements de soins et du personnel de santé qu'elle implique requerra une vigilance accrue pour tout ce qui concerne la protection des données et la sécurité informatique. «Les institution s'y mettent gentiment. Mais elles n'ont pas encore pris la mesure du problème».

Même constat pour Philine Richert chez Swisscom: «Beaucoup d'établissements ne disposent toujours que d'une protection de base.» Car le secteur social comme celui de la santé n'accordent encore que peu d'importance à la sensibilisation, à l'expertise et à la budgétisation de tout ce qui touche à la sécurité informatique. «Ce que nous constatons souvent en travaillant avec les professionnels de la santé, c'est qu'ils peinent à changer leurs habitudes», par exemple modifier régulièrement leur mot de passe, ou adopter l'authentification à double facteur. «Ce qu'on nous répond souvent, c'est que c'est difficile à intégrer dans le déroulement d'une journée-type.» Trop souvent, un établissement n'investit dans la prévention informatique qu'une fois qu'il a été victime d'une attaque.

En ce qui concerne le transfert sécurisé de données entre patients et personnel de santé, le baromètre d'eHealth Suisse de mars 2019 montre que la nécessité d'agir concerne tout particulièrement les EMS. Seuls 52 % des sondés admettent en effet échanger des données électroniques sur les soins de manière systématique, ou presque toujours, sécurisée, tandis que ce pourcentage s'élève à 87 % en milieu hospitalier.

**La sécurité des données exige expertise et investissement**

Conformément aux prescriptions légales, une protection adéquate commence, pour une entreprise, par l'identification de ses données sensibles et des droits d'accès qui y sont liés. Comme le souligne André Rotzetter, sous sa double casquette de spécialiste en cybersanté et de directeur d'institution: «Il faut que l'entreprise commence par s'assurer que certaines données ne sont lues et traitées que par des personnes autorisées.» Tout particulièrement dans le contexte d'interconnexion croissante entre les divers acteurs du domaine de la santé. Il s'agit ensuite d'identifier les risques et d'appliquer les mesures de sécurité qui s'imposent.

L'essentiel, selon les experts, c'est d'avoir une bonne infrastructure informatique. En font partie un pare-feu actualisé en permanence, un filtre anti-spam, et un programme de détection des virus qui soit vraiment capable de repérer et de neutraliser tous les virus connus. «Mais pour se protéger de manière efficace, il ne suffit plus aujourd'hui de simplement s'équiper d'un bon ordinateur», insiste Tobias Fessler, responsable de l'équipe informatique du centre de soins régional de Baden, également en charge du bon fonctionnement du système informatique de centre pour personnes âgées Kehl. «Pour qu'un système fonctionne convenablement, il faut une planification pérenne mais aussi des investissements réguliers.»

Outre les contrôles de sécurités permanents de la structure informatique et de chaque ordinateur, une bonne stratégie de sauvegarde est indispensable. Pour Tobias Fessler, elle ne doit pas se limiter à sécuriser les disques durs mais inclure aussi les serveurs. Parce qu'une cyberattaque peut complètement détruire un serveur. Bien sûr, ce genre de solutions de sauvegarde globale a un certain coût.

**Le danger des échanges par courriels**

Communiquer vers l'extérieur, avec d'autres professionnels de la santé – des médecins, mais aussi des proches de patients – requiert une vigilance particulière. On échange de moins en moins par fax – et par conséquent, l'échange d'informations, même entre professionnels, se fait de plus en plus souvent par e-mail. Pour s'assurer que les données sensibles des patients et des résidents sont envoyées en toute sécurité, il est indispensable que les courriels soient cryptés. Tous nos experts s'accordent sur ce point: envoyer des données de patients par e-mail non sécurisé est punissable.

Analyser les risques liés à la protection des données comme à la sécurité informatique – et prendre les mesures adéquates – exige expertise et investissement. Une institution dédiée à l'encadrement de personnes ayant besoin de soutien ne peut, la plupart du temps, assumer seule cette tâche: ses compétences sont ailleurs. André Rotzetter et l'association Altersbetreuung im oberen Fricktal ont choisi de coopérer avec un prestataire extérieur et renoncé à conserver un service informatique à l'interne. En tant qu'avocat spécialisé en informatique, Lukas Fässler plaide également en faveur d'une externalisation de tout ce concerne l'informatique: «L'avantage des contrats conclus avec des sociétés tierces est que ce sont elles qui sont responsables en cas de problèmes.» La mutualisation de l'informatique entre plusieurs institutions peut également constituer une alternative. C'est la solution choisie par le centre de soins régional de Baden et le centre pour personnes âgées Kehl.

Mais même les mesures de sécurité les plus pointues ne sont utiles que si les utilisateurs et les collaborateurs sont sensibilisés à ces questions. Les mails de hameçonnage (ou phishing) sont particulièrement dangereux car ils permettent aux cybercriminels de pénétrer à l'intérieur du système. Le maliciel se trouve dans la pièce jointe d'un message amusant ou alléchant: il suffit de l'ouvrir, ou parfois même simplement de cliquer sur le message lui-même, pour que le système tout entier soit infecté par un virus inconnu jusqu'alors. La règle est simple: ne jamais ouvrir les courriels d'expéditeurs inconnus, si amusants qu'ils puissent paraître! ●

Texte traduit de l'allemand

Annonce