Der Datenschutz und die Datensicherheit erfordern hohe Aufmerksamkeit : "Die Gefahr der Cyberkriminalität hat dramatisch zugenommen"

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

Objekttyp: **Article**

Zeitschrift: **Curaviva : Fachzeitschrift**

Band (Jahr): **90 (2019)**

Heft 6: **Digitalisierung : Chancen und Herausforderungen**

PDF erstellt am: **21.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-886013

Der Datenschutz und die Datensicherheit erfordern hohe Aufmerksamkeit

«Die Gefahr der Cyberkriminalität hat dramatisch zugenommen»

Institutionen im Gesundheits- und Sozialbereich befassen sich vielfach zu wenig mit Fragen der Datensicherheit. Die Cyberkriminalität sowie die zunehmende digitale Vernetzung zwingen zu umfassenden Massnahmen. Es genügt heute nicht mehr, einfach einen guten Computer hinzustellen.

Von Elisabeth Seifert

Selbst eine IT-Infrastruktur auf dem neuesten Stand der Technik ist nicht immer vor Trojanern und Co. gefeit. Diese Erfahrung machte André Rotzetter. Er berät Pflegeeinrichtungen rund um das Thema eHealth und ist Geschäftsführer des Vereins Altersbetreuung im oberen Fricktal AG mit zwei Pflegeeinrichtungen für über 200 ältere Menschen. Trotz Firewall samt ausgeklügeltem Virenschutzprogramm bahnte sich dort ein Schädling einen Weg ins Computersystem: Auch die besten Schutzprogramme erkennen immer nur die bereits bekannten Viren.

Der (noch) unbekannte Eindringling sass auf der PDF-Datei, die ein Stellenbewerber seiner eMail angehängt hatte. Kaum hatte André Rotzetter den Anhang geöffnet, spielte das System verrückt. Da half nur noch eines: «Um einen grösseren Schaden zu verhindern, haben wir sofort alle Computer vom Netz genommen», erinnert er sich – und der Schaden blieb gering. Für solche Fälle hat seine Einrichtung nämlich vorgesorgt: Jeden Mittag wird ein internes Backup sämtlicher Daten und Transaktionen erstellt. Und jeden Abend werden diese dann auf den externen, hochsicheren Server einer darauf spezialisierten Firma transferiert. Auf diese Weise gehen bei einem Hacker-Angriff maximal die Transaktionen eines halben Tages verloren.

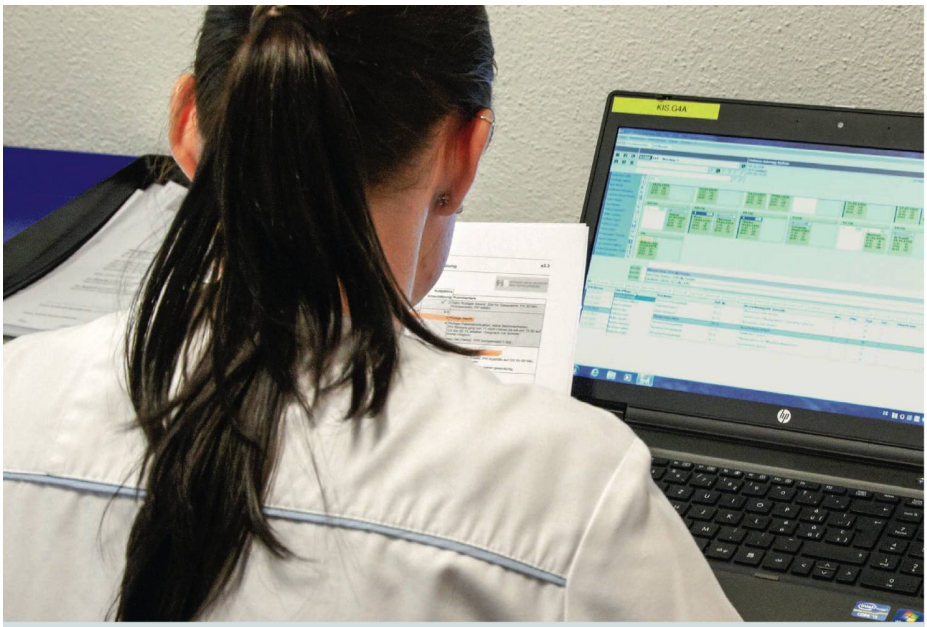
«Die Angriffe sind in aller Regel nicht gezielt auf einzelne Betriebe ausgerichtet.»

Weniger gut gewappnet für einen Cyberangriff war das regionale Alterszentrum im aargauischen Schöftland. Der Fall sorgte im Dezember 2017 für Schlagzeilen. Eine Schadsoftware verschlüsselte dort innert Kürze digital abgelegte Daten der über 100 Bewohnerinnen und Bewohner – und diese waren, vorerst, verloren. Erst nachdem die Institution den Cyberkriminellen ein Lösegeld bezahlt hatte, wurden die Daten freigegeben.

Digitalisierung sensibilisiert für den Datenschutz

Diese beiden Hacker-Angriffe auf Pflegeeinrichtungen sind keine Einzelfälle. Zahlreiche Betriebe in der Schweiz, auch aus dem Gesundheits- und Sozialbereich, waren schon einmal Ziel solcher Attacken. «Die Gefahr der Cyberkriminalität hat dramatisch zugenommen», sagt der auf Datenschutz- und Datensicherheitsfragen spezialisierte Rechtsanwalt Lukas Fässler. Einrichtungen im Gesundheits- und Sozialbereich seien dabei besonders von zwei Tatmotiven betroffen: Zum einen lasse sich mit dem Verkauf abgesaugter Patientendaten gutes Geld machen, und zum anderen werden Institutionen – wie im Fall des Heims in Schöftland – erpressbar, wenn Viren das System zum Absturz bringen.

Die Gefahr von Cyberangriffen, gerade auch auf kleinere und mittlere Betriebe im Sozial- und Gesundheitsbereich, sei definitiv real, betont auch Philine Richert. Sie ist Chief Information Security Officer bei Swisscom Health, einer Tochtergesellschaft von Swisscom, die digitale Lösungen für das Gesundheitswesen anbietet. Die Angriffe seien in den allermeisten Fällen nicht gezielt auf eine einzelne Institution ausgerichtet, um dort Schaden anzurichten. Die Angreifer führen vielmehr eine grosse Zahl von Versuchen aus, in möglichst viele Systeme einzudringen. Auf eine erfolgreiche Attacke folge dann oft eine Geldforderung, um beispielsweise verschlüsselte Daten wieder freizugeben.



Damit sich möglichst keine Schadsoftware im System festsetzt, braucht es eine Sensibilisierung jeder Mitarbeiterin und jedes Mitarbeiters. Foto: Martin Glauser

Von Bedeutung für die betroffenen Betriebe seien dabei längst nicht nur die finanziellen Auswirkungen. In konkreten Fällen mussten etwa Kliniken und Spitäler Behandlungen oder Operationen verschieben, so Philine Richert. Und in Pflegeeinrichtungen könne es dazu kommen, dass digitale Medikations- und Pflegepläne nicht mehr abgerufen werden können. Abgesehen davon, dass Hacker-Angriffe den Behandlungs- und Pflegeprozess beeinflussen können, sind gerade im Gesundheits- und Sozialbereich immer schützenswerte Personendaten betroffen. Der Imageschaden für die betroffenen Einrichtungen ist riesig, wenn solch sensible Daten wegkommen oder manipuliert werden. Mit der zunehmenden Digitalisierung aller administrativen und pflegerischen Belange kommt den Fragen des Datenschutzes und der Datensicherheit eine wachsende Bedeutung zu.

Der Imageschaden ist riesig, wenn sensible Daten wegkommen oder manipuliert werden.

Die Herausforderungen einer digitalisierten Gesellschaft im Bereich Datenschutz und die Datensicherheit schlagen sich auch in verbindlicheren rechtlichen Regelungen nieder. In der EU sind letztes Jahr Bestimmungen in Kraft getreten, die längst bestehendem Recht endlich Geltung verschaffen sollen. Und wie Datenschutzexperte Lukas Fässler ausführt, dürften solche Bestimmungen auch in die zurzeit laufende Totalrevision des Schweizer Datenschutzgesetzes einfliessen. Im EU-Raum müssen Betriebe mithilfe von Dokumenten nachweisen können, dass sie die Datenschutzbestimmungen einhalten. Zu diesem Zweck sind sie verpflichtet, eine verantwortliche Person zu benennen. Diese sorgt dafür, dass ein Dateninventar erarbeitet wird, welche schützenswerten Personendaten wo und wie abgelegt werden. Dabei muss auch geklärt sein, wer welche Aktivitäten im Rahmen der Verarbeitung der Daten ausführt.

Zudem braucht es eine Beurteilung der Risiken, welche mit der Bearbeitung dieser Personendaten eintreten könnten. Schliesslich müssen Massnahmen definiert werden, wie sich diese Risiken minimieren lassen. «Bereits heute besteht die Verpflichtung, schützenswerte Daten zu inventarisieren und Massnahmenpläne sicherzustellen, aber nur wenige Datenverarbeiter machen das auch konsequent», kritisiert Fässler. «Das Datenschutzgesetz ist oft leider noch Makulatur.»

«Heime machen sich langsam auf den Weg»

Vor dem Hintergrund der zunehmenden Cyberkriminalität werde die Öffentlichkeit für solche Fragen jedoch sehr stark sensibilisiert, beobachtet Fässler. Und bei den Pflegeeinrichtungen steige das Interesse zudem im Hinblick auf die gesetzlich verankerte Pflicht, sich bis 2022 dem elektronischen Patientendossier (EPD) anzuschliessen. Die damit einhergehende digitale Vernetzung von Gesundheitseinrichtungen und Gesundheitsfachpersonen zwingen zu einer noch höheren Aufmerksamkeit gegenüber allen Belangen des Datenschutzes und der Datensicherheit. «Die Heime machen sich langsam auf den Weg», sagt Lukas Fässler, «sie befassen sich aber noch nicht genügend mit solchen Fragen.» Diese Erfahrung macht auch Philine Richert von der Swisscom. >>

«Viele Häuser verfügen über einen Grundschutz, aber über nicht viel mehr.» Auf das Bewusstsein, Know-how und auch das Budget bezüglich IT-Sicherheit werde im Gesundheits- und Sozialbereich eher weniger Wert gelegt. «Wir erleben im Kontakt mit Gesundheitsfachpersonen häufig, dass sie nur schwer zu einer Verhaltensänderung zu bewegen sind.» Dies betreffe etwa die Empfehlung, regelmässig das Passwort zu ändern, oder eine Zwei-Weg-Authentifizierung zu nutzen. «Sie entgegnen uns oft, dass sich dies nur schwer in ihren Tagesablauf integrieren lasse.» Oft werde erst dann in die Prävention investiert, wenn man bereits Opfer eines Cyberangriffs geworden ist.

«Ein Betrieb muss sicherstellen, dass bestimmte Daten nur jene lesen, die dazu befugt sind.»

Was den gesicherten Datentransfer zwischen Patienten und Gesundheitsfachpersonen betrifft, legt der Swiss-eHealth-Barometer vom März 2019 insbesondere bei den Pflegeeinrichtungen Handlungsbedarf offen: Nur 52 Prozent der Befragten geben an, dass der elektronische Austausch über die Behandlung immer oder meistens gesichert erfolgt, zum Beispiel über verschlüsselte eMails. Bei den Spitälern liegt der Anteil bei hohen 87 Prozent.

Datensicherheit erfordert Know-how und Investition

Entsprechend den gesetzlichen Bestimmungen fängt ein guter Datenschutz damit an, dass sich ein Betrieb bewusst macht, über welche schützenswerten Daten er verfügt und wer darauf Zugriff haben soll. «Es muss innerhalb eines Betriebs sichergestellt sein, dass bestimmte Daten nur von jenen gelesen und weiterverarbeitet werden können, die das auch wirklich dürfen», betont eHealth-Spezialist und Heimleiter André Rotzetter insbesondere mit Blick auf die zunehmende Vernetzung der Akteure im Gesundheitswesen. Weiter gelte es, die Risiken aus Sicht des Datenschutzes und der Datensicherheit zu benennen – und die entsprechenden Sicherheitsmassnahmen einzuleiten.

Zentral ist für die Experten dabei eine gute IT-Infrastruktur. Zum Pflichtprogramm gehören eine ständig aktualisierte Firewall, der Anti-Spam-Filter sowie ein Viren-Scanning-Programm, das auch wirklich alle – bekannten – Computerschädlinge dingfest machen und ausschalten kann. «Um für alle Gefahren gerüstet zu sein, genügt es heute aber nicht mehr, einfach einmalig einen guten Computer hinzustellen», unterstreicht Tobias Fessler, Leiter des Informatikteams des Regionalen Pflegezentrums Baden. Gemeinsam mit seinen Teamkollegen ist er zudem für das reibungslose Funktionieren der digitalen Systeme im Alterszentrum Kehl zuständig. «Damit ein System stabil ist, braucht es eine nachhaltige Planung und auch laufende Investitionen.»

Neben der ständigen sicherheitsrelevanten Überprüfung der Gesamtstruktur sowie der einzelnen Geräte ist etwa auch eine gute Backup-Strategie erforderlich. Gemäss Tobias Fessler darf sich eine solche Strategie nicht nur auf die Absicherung der Datenlaufwerke beziehen, sondern muss auch die Serversysteme einschliessen. Ein Cyberangriff kann nämlich auch ganze Server zerstören. Solch umfassende Backup-Lösungen sind freilich nicht ganz billig.

Besondere Aufmerksamkeit erfordert die Kommunikation nach aussen, mit anderen Gesundheitsfachpersonen, etwa Ärzten, aber auch mit Angehörigen. Weil der Austausch über Fax immer seltener wird, gewinnt die eMail-Kommunikation gerade auch im Austausch mit Fachpersonen derzeit an Bedeutung. Damit der Versand schützenswerter Patienten- oder Bewohnerdaten per Mail gesichert erfolgt, müssen solche Mails verschlüsselt werden. Wer Patientendaten mit ungesicherten Mails verschickt, mache sich strafbar, sind sich die Experten einig.

Die Risiken rund um das Thema Datenschutz und Datensicherheit zu analysieren und die nötigen Massnahmen einzuleiten, erfordert Know-how und Investitionen. Eine Einrichtung alleine kann das häufig nicht mehr stemmen, zumal die Kernkompetenzen der Institutionen für Menschen mit Unterstützungsbedarf auf anderen Gebieten liegen. André Rotzetter und der Verein für Altersbetreuung im oberen Fricktal haben sich für die Zusammenarbeit mit einem externen Dienstleister entschieden – und verzichten auf eine eigene IT-Abteilung. Zu einer Auslagerung der IT-Bereichs an professionelle Service-Dienstleister rät etwa

«Verträge mit Drittfirmen haben den Vorteil, dass diese haftbar gemacht werden können.»

Wie sicher ist das elektronische Patientendossier?

Ab April 2022 müssen alle Pflegeeinrichtungen in der Schweiz und Institutionen für Menschen mit Behinderung, die über die Krankenkasse abrechnen, Daten ihrer Bewohnerinnen und Bewohner auf Wunsch über ein elektronisches Patientendossier (EPD) zugänglich machen. Im Spitalbereich besteht diese Verpflichtung bereits ab April 2020. Die im EPD abrufbaren Daten verbleiben grundsätzlich in den primären Datensystemen der Leistungserbringer, also der Heime, der Spitäler oder auch der Hausärzte. Das EPD speichert keine Daten, es vernetzt die Datenablagen vielmehr untereinander, ruft die Daten im Moment der Abfrage ab und zeigt diese an. Diese Vernetzung läuft über eine eHealth-Plattform. Die beiden grössten Plattform-Betreiber in der Schweiz sind die Swisscom und die Post. Die einzelnen Leistungserbringer sind über ihre Mitgliedschaft bei einer Gemeinschaft oder Stammgemeinschaft, die technische und organisatorische Dienstleistungen erbringt, an eine eHealth-Plattform angeschlossen.

Während der Kontakt zu den Leistungserbringern und den Patienten grundsätzlich in der Verantwortung der Stammgemeinschaften liegt, sind die Plattform-Betreiber als technische Anbieter zuständig für den reibungslosen Betrieb und das Störungsmanagement der eHealth-Plattform und des EPD. Wie die Post auf Anfrage der Fachzeitschrift schreibt, garantiere sie den Stammgemeinschaften, dass das EPD zertifizierbar ist. Die Stammgemeinschaften – und damit indirekt auch die Plattformbetreiber – werden in den kommenden Monaten im Auftrag des Bundes auf Herz und Nieren geprüft. Sicherheitsfragen stehen dabei ganz weit oben. Sowohl die Swisscom als auch die Post bekennen sich zu höchsten Sicherheitsvorkehrungen. Die Datenvernetzung erfolgt in modernsten Rechenzentren in der Schweiz.

Zu den Sicherheitsvorkehrungen gehört zum Beispiel, dass Patientinnen und Patienten sowie die Gesundheitsfachpersonen eine digitale Identität benötigen, um das EPD zu nutzen. Diese digitale Identität erhalten sie bei Identitätsprovidern. Um für das EPD zugelassen zu werden, müssen sich die Identitätsprovider vom Bund zertifizieren lassen. Eine weitere gesetzliche vorgeschriebene Sicherheitsmassnahme ist ein starkes Login mittels einer Zwei-Faktor-Authentifizierung. Zudem bestimmen die Patienten selber, welchen Institutionen und Fachpersonen sie den Zugriff auf ihr EPD ermöglichen und für wie lange sie den Zugriff erteilen. Eine Ausnahme gibt es: Im medizinischen Notfall kann eine Fachperson auch ohne Zugriffsrechte die Dokumente einsehen.

Trotz allen Sicherheitsvorkehrungen könne ein kriminell motivierter Angriff im IT-Bereich nie gänzlich ausgeschlossen werden, heisst es vonseiten der Post. Im Fall des EPD müsste die Täterschaft aber sowohl die elektronische Identität eines Patienten fälschen als auch die Zwei-Faktor-Authentifikation überwinden.

auch Informatikanwalt Lukas Fässler: «Verträge mit Drittfirmen haben zudem den Vorteil, dass diese haftbar gemacht werden können, wenn etwas schiefläuft.» Eine Alternative zur Zusammenarbeit mit externen Profis besteht in einer auf den IT-Bereich bezogenen Kooperation mehrerer Institutionen. Ein Weg, den das Regionale Pflegezentrum Baden und das Alterszentrum Kehl gewählt haben.

Auch die besten Sicherheitsmassnahmen können ihre Wirkung allerdings nur dann voll entfalten, wenn die Nutzerinnen und Nutzer, der Mitarbeiter und die Mitarbeiterin, für die entsprechenden Fragen sensibilisiert sind. Eine besondere Gefahr stellen Phishing-Mails dar, mit denen sich Cyberkriminelle oft Zugang zu einem Computersystem verschaffen wollen. Die Schadsoftware sitzt dabei auf dem Anhang eines Mails mit einem verlockenden, lustigen Inhalt oder einer üblichen Postzustellung wie Bewerbungsunterlagen. Öffnet man den Anhang (manchmal genügt auch schon nur das Mail) ist das System mit einem – bis jetzt unbekannten – Virus sofort infiziert. Mails von unbekannten Absendern, mögen diese auch noch so lustig sein, sollten deshalb nicht geöffnet werden. ●