# HEIME UND SPITÄLER

Fachzeitschrift
für Geschäfts- und Pflegeleitung,
Küchenchefs, Verantwortliche
Haustechnik und Einkauf

Nr. 2
Mai 2018



**8 Ausbildung**
Einzigartiges Pflege-Schul-konstrukt – das Interview

**11 Facility Management**
Mit dem Logistik-Masterplan neue Wege beschreiten

**24 Gesundheitsmarkt**
Die Zukunft der Pflege-Organisation in Spitälern

Wirtschaftlichkeit steigern

## Fokus Prozessküche

Seite 42

Spezialsortiment für die
CARE-GASTRONOMIE
transgourmet.ch/care-shop

TRANSGOURMET

# Cyber-Risiken ernst nehmen

**Im Frühjahr 2020 werden schweizweit das elektronische Patientendossier (EPD) sowie ein Portal für Gesundheits-Informationen eingeführt. Doch was ist, wenn Login oder andere Daten der Gesundheitsdienstleister und Patienten verloren gehen oder gar in falsche Hände geraten?**

*Melanie Koller[1], Frank von Saal[2]*

Das Geschäft mit Gesundheitsdaten ist lukrativ. Auf dem Schwarzmarkt sind sie sogar um ein Vielfaches wertvoller als Kreditkartendaten. Dies erstaunt nicht, denn ein Grossteil der Industrie entwickelt anhand von Gesundheitsdaten individualisierte Produkte wie Medikamente, Lebensmittel oder Sportartikel. Deshalb sind Gesundheitsdaten lohnende Ziele für Cyber-Kriminelle. Die Gesundheitsbranche ist aufgrund der zunehmenden digitalen Vernetzung, ungeschützter Medizinalgeräte und veralteter IT-Infrastruktur häufig mit Cyber-Vorfällen konfrontiert. Hinzu kommt der Faktor Mensch: In Heimen, Spitälern usw. wird in Schichten gearbeitet, was eine Kontrolle des Datenverkehrs erschwert.

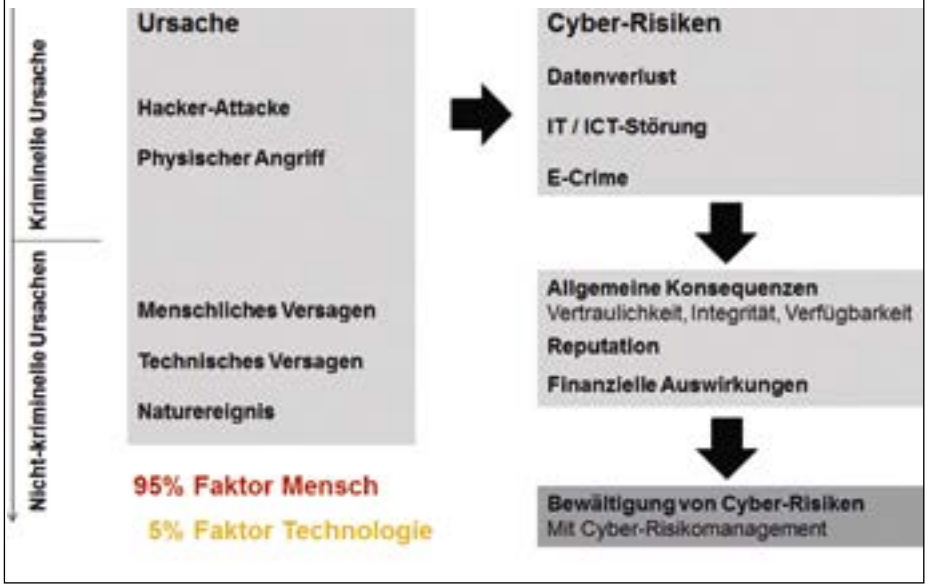
### Gravierende Vorfälle

Neben der Cyber-Angriffswelle Mitte 2017 kam es beispielsweise zu zwei symptomatischen Cyber-Erpressungen, auf die unterschiedlich reagiert wurde: In das IT-System des Regionalen Alterszentrums Schöftland im Aargau wurde Ende 2017 ein Trojaner eingeschleust – die Erpresser forderten als Lösegeld einen Bitcoin im Wert von 7800 US-Dollar. Der Betrag war gering, doch der vermeintlich immaterielle Schaden war hoch. Die Heimleitung zahlte, damit die verschlüsselten Daten wieder zugänglich waren. Das Altersheim hatte Glück im Unglück, denn eine Garantie für die Entschlüsselung gibt es nicht, auch wenn man auf eine Erpressung eingeht. Anders hatte 2016 das deutsche Lukaskrankenhaus in Neuss reagiert: Durch das Anklicken eines E-Mail-Anhangs gelangte ein Trojaner ins IT-System und verschlüsselte diverse Dateien, bevor das System heruntergefahren werden konnte. Das Lukaskrankenhaus bezahlte nicht, da es auf ein Backup vom Vorabend des Angriffs zurückgreifen konnte. Doch es wurde für eine halbe Woche um 30 Jahre zurückversetzt und musste dafür teuer bezahlen: Insgesamt kostete der Kampf gegen den Trojaner rund 1,2 Millionen Franken. Immerhin: Durch verschiedene zusätzliche Massnahmen ist das IT-System heute wesentlich sicherer.

### Die Meldepflicht kommt

In der Schweiz gibt es derzeit keine gesetzliche Pflicht, Datenpannen oder Datensicherheitsvorfälle wie die genannten Erpressungsfälle den Betroffenen oder den Datenschutzbehörden zu melden. Zu beurteilen, ob und in welcher Quantität Cyber-Schäden in Heimen und Spitälern vorkommen, ist deshalb nur anhand von Zahlen aus dem nahen Ausland zu schätzen. Mit der 2. Revision des Schweizer Datenschutzgesetzes (E-DSG) ist jedoch eine deutliche Richtungsänderung vorgesehen, was hoffentlich zu mehr Transparenz bei Cyber-Schadenvorfällen führt.

**Cyber-Risk und der Faktor Mensch**




### Beispiel elektronisches Patientendossier

Der Entwurf des revidierten E-DSG, das frühestens Ende 2018/Anfang 2019 in Kraft tritt, enthält eine gesetzliche Meldepflicht für jegliche Verletzung der Datensicherheit – unabhängig von der Absicht oder Widerrechtlichkeit, die zum Vorfall führt, der ein hohes Risiko für die Betroffenen bezüglich Persönlichkeit oder Grundrechte darstellt. Zunächst muss der Eidgenössische Daten- und Öffentlichkeitsbeauftragte (EDÖB) informiert werden. Die Betroffenen müssen erst benachrichtigt werden, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB dies verlangt. Auf dem Datenportal des EPD wer-

den Kopien der Patientendokumente gespeichert. Die Originale bleiben immer beim Patienten, der als Administrator bestimmen kann, welche Institutionen und Gesundheitsfachpersonen Zugriff darauf haben. Die Zugangsportale für die Gesundheitsfachpersonen führen mit einem Login direkt zum EPD. Werden bei einem Hacker-Angriff Zugangsdaten zum EPD gestohlen oder manipuliert, kann dies für einen Patienten schwerwiegende Konsequenzen haben. In einem solchen Fall ist davon auszugehen, dass die verantwortliche Gesundheitsinstitution den Patienten persönlich benachrichtigen muss, damit dieser sämtliche offenen Zugriffe sperren und sich schützen kann.

## Hohe finanzielle Risiken

Die Kosten solcher Datensicherheitsverletzungen können auch in der Schweiz hoch sein. Neben den Kosten für die Benachrichtigung der Betroffenen entstehen auch regulatorische Verfahrenskosten und möglicherweise Zahlungen aufgrund von Schadenersatzansprüchen Dritter infolge Persönlichkeitsverletzungen. Benachrichtigungskosten beispielsweise entstehen durch den Aufwand zur Erstellung der Kontaktdaten, Ermittlung der regulatorischen Anforderungen und Einschaltung externer Experten wie etwa Kommunikationsfachleuten.

Gemäss einer Studie des Ponemon Institute aus den USA beliefen sich allein die Benachrichtigungskosten in Deutschland pro Unternehmen auf durchschnittlich 200 000 Franken. Hohe Kosten entstehen ebenfalls für das Krisenmanagement, etwa für IT-Forensik, Datenschutzspezialisten und PR-Beratung. Auch die Wiederherstellung und Ersatzbeschaffung von Daten und Systemen sowie damit einhergehende Betriebsunterbrüche erzeugen Kosten. Angesichts der Entwicklung der Cyber-Risiken schliessen heute immer mehr Institutionen des Gesundheitswesens Cyber-Versicherungen ab. Das kann durchaus sinnvoll sein, denn Cyber-Risiken sind heute vielfach Top-Unternehmensrisiken, weshalb der Abschluss solcher Versicherungen früher oder später auch in der Schweiz Standard werden wird. ■

*[1] Legal Counsel Cyber Risk bei Kessler & Co AG*

*[2] Kundenberater bei Kessler & Co AG*

***Referenzen***

*https://www.e-health-suisse.ch/elektronisches-patientendossier.html>, Stand: 05.04.2018.*

*https://www.althammer-kill.de/news-detail/gesundheitsdaten-sind-wertvoller-als-finanzdaten/, Stand: 05.04.2018.*

*https://www.aargauerzeitung.ch/aargau/wyna-suhre/cyber-angriff-altersheim-liess-sich-erpressen-und-zahlte-polizei-erst-nach-gelduebergabe-informiert-132016353>, Stand: 05.04.2018.*

*https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html>, Stand: 05.04.2018.*

*Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Er-lasse zum Datenschutz Art. E-DSG 22, S. 128 f.*

Plateforme pour la chimie,
la pharmacie et la biotechnologie

ILMAC
LAUSANNE

3. und 4. Oktober 2018 | Expo Beaulieu Lausanne

Für die französischsprachige Schweiz

Partner

VAUD

SCG Schweizerische Chemische Gesellschaft | SSC Société Suisse de Chimie | SCS Swiss Chemical Society

bioalps

scienceINDUSTRIES SWITZERLAND

Swiss Biotech Association

SCV Schweizerischer Chemie- und Pharmaberufe Verband