

Nehmen Gesundheitsinstitute den Datenschutz genug ernst?

Datenschutz: Jeder ist ein Beschützer

«Niemand hat Freude an Vorschriften», stellte Urs Achermann, Chief Information Security Officer der HINT AG, an den Anfang seiner Betrachtungen. «Aber sie sind im Datenschutz von elementarer Bedeutung. Leider ist im Gesundheitswesen das Bewusstsein für Datenschutzfragen vielerorts sehr schlecht ausgeprägt. Das erstaunt mich immer wieder, wenn man bedenkt, wie sensibel die Daten sind, mit welchen täglich gearbeitet wird. Es lohnt sich daher sehr, die Mitarbeitenden vorbeugend im korrekten Umgang mit diesen Daten zu schulen.»

Gerade im Gesundheitswesen mit seinen hochsensiblen Patientendaten kann dem Schutz der Daten nie zu viel Bedeutung beigemessen werden. Patientendaten sind sozusagen die Kronjuwelen der Gesundheitsinstitute: es gibt keine Daten, die höhere Sicherheitsmassnahmen verlangen. Das Bewusstsein im sicheren Umgang mit diesen besonders schützenswerten Personendaten ist daher ein absolut entscheidender Punkt. Denn mit

Urs Achermann, Chief Information Security Officer HINT AG, bezeichnete die meist sensiblen Patientendaten als Kronjuwelen, die eines ganz besonders ausgefeilten Datenschutzes bedürfen.

technischen Mitteln alleine ist es nicht getan, Datensicherheit und Datenschutz wird letztlich auch stark durch den Faktor Mensch bestimmt.

Beispiele aus der Praxis – Risiken werden wenig beachtet

«Es gibt auch Beispiele von guten Beschützern», zeigte Urs Achermann auf. «Eine Mitarbeiterin eines Kunden regte an, die automatische Sperrung des Bildschirms von 15 auf 3 Minuten Inaktivität zu reduzieren. Viele Mitarbeitende in einem Spital werden immer wieder zu einem Patienten gerufen und müssen deshalb ihren Büroarbeitsplatz schnell verlassen.» Leider seien die guten Beispiele wesentlich rarer als die negativen Beispiele. So komme es immer wieder vor, dass Benutzer ihre Passwörter nicht periodisch ändern wollen oder den Wunsch äussern, diesen Schutz vollständig zu deaktivieren. «Diese Leute haben nicht verstanden, dass ein Passwort kein Hindernis, sondern ein praktischer Zugriffsschutz auf die Patientendaten darstellt», unterstrich Achermann. Ebenso kämpft er vehement gegen Gruppen-Accounts im Spital: «Der Datenschutz verlangt eine lückenlose Rückverfolgbarkeit im Einsehen oder Gebrauch von besonders schützenswerten Personendaten. Mit einem Gruppen-Account kann man aber nie belegen, wer effektiv auf die Daten zugegriffen hat. Dies kann erhebliche rechtliche Folgen für den Leistungserbringer nach sich ziehen.»

Es kommt noch schlimmer: In einem anderen Beispiel verlangte ein externer Softwarelieferant die Herausgabe einer kompletten Datenbank-Sicherung, um eine Störungsmeldung aufspüren zu können. «Hätten wir dies getan, lägen alle Daten von Patienten, Mitarbeitenden und Ärzten dieses Institutes ungeschützt bei dieser Softwarefirma. Stellen Sie sich vor, der Software Entwickler würde diese Daten dann auf seinen Laptop kopieren, um auch unterwegs daran zu arbeiten. Auf dem gleichen PC amüsiert sich dann am Abend seine ganze Familie mit digitalen Spielen. Und das worst case Szenario: ein paar Monate später wird der Laptop auf ricardo.ch versteigert! Das wäre die Datenschutz-Katastrophe für das betroffene Institut. Solche Mitarbeitende sind schlechte Beschützer.»

Wie wird man ein guter Beschützer?

«Üben, üben und nochmals üben», lautet des Sicherheits-Fachmanns Rat. «Es beginnt damit, dass im Spital ein Datenschutz-Verantwortlicher bestimmt wird. Es muss eine Persönlichkeit sein, die mit den gesetzlichen





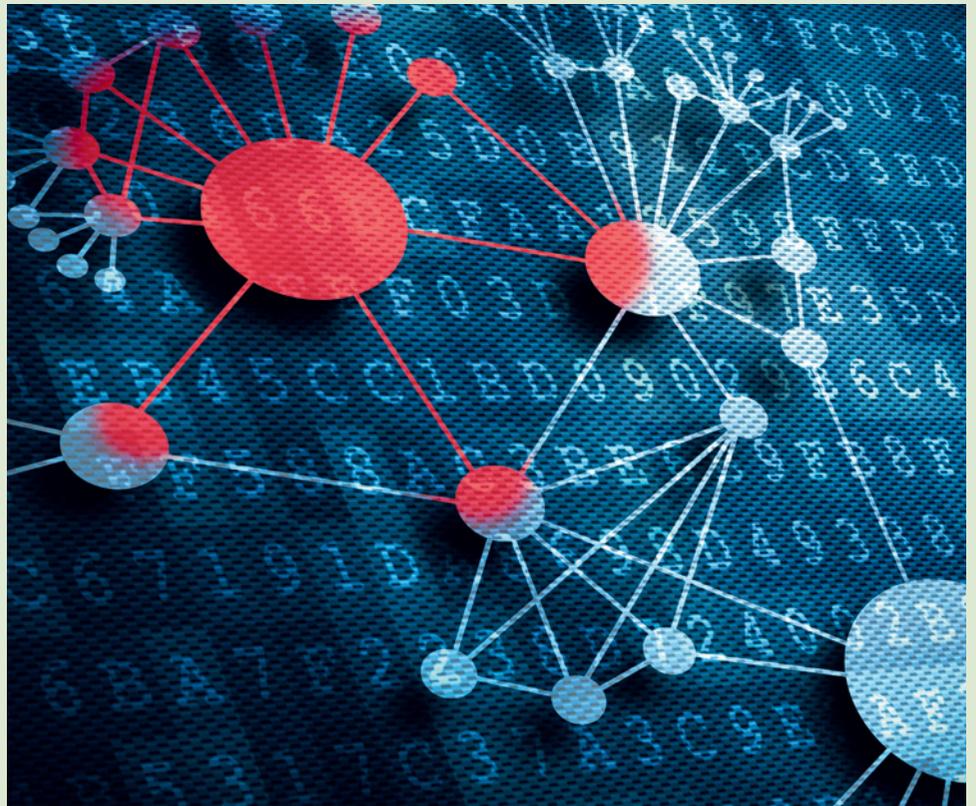
Urs Achermann, Chief Information Security Officer, HINT AG

Auflagen vertraut ist sowie die technischen Möglichkeiten und die Besonderheiten des Gesundheitswesens kennt. Zweitens muss dieser Verantwortliche mit den nötigen Befugnissen ausgestattet sein. Das heisst: Anlaufstelle sowie verantwortliches Freigabe- und Kontrollorgan. Drittens müssen von hier aus regelmässige Schulungen der Mitarbeitenden initiiert werden.»

Phantasie ist dabei wertvoll. Ein kluges wie witziges Plakat, Flyer fürs Personal oder Infos an Orten, die häufig aufgesucht werden – etwa bedruckte Kaffeebecher in der Cafeteria – könnten Gold wert sein. «Die Mitarbeitenden müssen Datenschutz verstehen lernen», so Achermann, «nur so können sie die ihnen anvertrauten Daten auch angemessen beschützen.»

Schliesslich komme es auf die Umsetzung in der täglichen Praxis an: «Der Datenschutzverantwortliche muss die Handhabung regelmässig kontrollieren, Fehler aufzeigen, aber nicht schulmeisterlich wirken oder gar bestrafen. Es geht vielmehr darum, Positives zu belohnen und generell alle Mitarbeitenden zu sensibilisieren und zu motivieren, den Datenschutz ernst zu nehmen und so aktive Beschützer zu werden.»

Text: Dr. Hans Balmer



Datenschutz ist wichtig – informieren Sie sich

Informationssicherheit wird immer wichtiger. Gerade im Gesundheitswesen mit seinen hochsensiblen Patientendaten kann dem Schutz der Daten gar nicht zu viel Bedeutung beigemessen werden. Viele Institutionen im Gesundheitswesen sind sich im Unklaren darüber, was es in Bezug auf die Sicherheit und den Schutz der Daten zu beachten gilt. Erfahren Sie im Rahmen eines umfassenden und praxisnahen Seminars alles Wissenswerte über die verschiedenen Aspekte des Datenschutzes und stellen Sie ihre eigenen kritischen Fragen.

Zeit

Donnerstag, 24. September, 8.30 bis 16.30 Uhr

Ort

HINT AG, Gebäude «Im Flügel», Niederlenzer Kirchweg 4, Lenzburg (ehemaliges Hero Gelände)

Programm

- Einführung in die Grundsätze des Datenschutzes
- Datenschutz in der klinischen Praxis
- Datensicherheit und IT-Hilfsmittel
- Fallbearbeitung
- Aktuelles zum Datenschutz aus der Gesundheitsdirektion des Kantons Aargau
- Datenschutz und Finanzen

Referenten

- lic. iur. RA Judith Naef, Judith Naef Rechtsanwälte AG, Zürich und Baar-Zug
- lic. iur. RA Roger Lehner, Departement Gesundheit und Soziales Kanton Aargau
- Urs Achermann, Chief Information Security Officer HINT AG

Anmeldung

www.hintag.ch oder per Email an events@hintag.ch

Kosten

CHF 590.–