

Schon einfache Maßnahmen können helfen

IT-SICHERHEIT UND DATENSCHUTZ ALS ANGEWANDTES QUALITÄTSMANAGEMENT

Das Gefährdungspotential im Bereich IT-Sicherheit und Datenschutz hat Hans-Georg Hunger wachgerüttelt. In punkto Datenschutz und IT-Sicherheit tut sich daher einiges bei der Kreiskrankenhaus Greiz GmbH.

„Risiken kann man aussitzen oder vorbeugen“, weiß Hans-Georg Hunger, Geschäftsführer der Kreiskrankenhaus Greiz GmbH. „IT-Sicherheit und Datenschutz bilden einen wesentlichen Bestandteil des Qualitätsmanagements bei Kliniken und somit auch für das Kreiskrankenhaus Greiz und entscheidet heute mit im Wettbewerb um die Dienstleistungen am Patienten. Bisher beschäftigen sich lediglich 30 Prozent aller Kliniken ernsthaft mit diesen Themen, dies sind zu wenige!“ Das Kreiskrankenhaus Greiz hat vor drei Jahren mit umfassenden Maßnahmen im Qualitätsmanagement begonnen und unter anderem die Zertifizierung durch die Joint Commission erfolgreich abgeschlossen. Wesentlicher Bestandteil dieser Zertifizierung sind die Qualitätsstandards in den Bereichen IT Sicherheit und Datenschutz. Dies hat Hans-Georg Hunger veranlasst, das Gefährdungspotential im Bereich IT-Sicherheit und Datenschutz einer eingehenden Prüfung zu unterziehen. Dabei war nicht unerheblich, dass auch die aktuelle Gesetzeslage die Krankenhausleitung im Rahmen des „Organisationsverschuldens“ stärker als bisher in die Pflicht nimmt. Kliniken und deren Leitung, die in punkto Datenschutz und IT-Sicherheit nicht ausreichend vorsorgen, sind in Schadensfällen haftbar.

Risiken bei IT-Sicherheit und Datenschutz sind dramatisch gewachsen

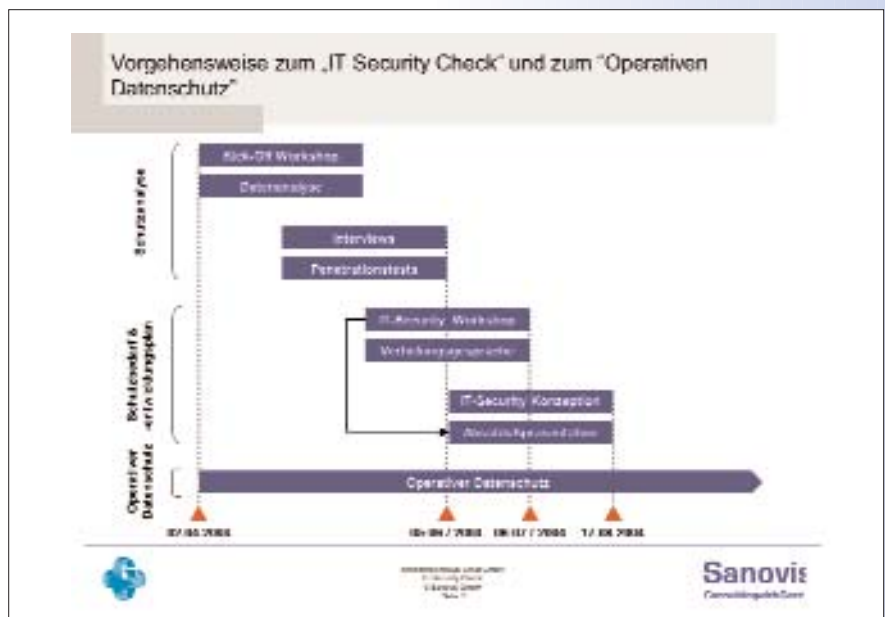
Die elektronische Patientenakte hat in vielen Kliniken Einzug gehalten und die Vernetzung zwischen Medizin, Pflege und Krankenhausverwaltung hat deutlich zugenommen. Neue Herausforderungen stehen mit der Einführung der Gesundheitskarte und der Health Professional Card für die Krankenhaus-IT bereits an. Viele Kliniken wären bei Ausfall der IT-Systeme nicht mehr handlungsfähig, der Handlungsbedarf im Bereich IT-Sicherheit und Datenschutz ist enorm! Doch dabei sollten nicht alleine Vorkehrungen gegen Viren und Hacker getroffen werden. „Das Thema interne Sicherheit wird vielfach vernachlässigt“, betont Uwe Günther, Geschäftsführender Gesellschafter der Sanovis GmbH. „Durchschnittlich 80 Prozent aller Sicherheitsbudgets fließen in Maßnahmen gegen Zugriffe von außen, gleichzeitig aber entstehen schätzungsweise 80

Prozent aller Schäden durch klinikinternen Fehlbenutzung oder Missbrauch“, sagt Uwe Günther. Im Fall der Kreiskrankenhaus Greiz GmbH war dies nicht anders. „Die Anzahl der IT-Nutzer hat sich mit der Einführung unseres Krankenhaus-Informationssystems in den letzten Jahren vervielfacht. Somit kommen immer mehr Mitarbeiter mit hoch sensiblen Patientendaten in Berührung. Die damit einhergehenden Probleme, wie die restriktive Vergabe von Zugriffsrechten, das durchgängige Verwenden von Bildschirmchonern und automatischen Bildschirmsperren mit Passwort oder das Bereitstellen einheitlicher Regelungen im Umgang mit E-Mail und Internet, werden einem oft erst nach einiger Zeit der Anwendung der Systeme bewusst“, so Hans-Georg Hunger.

Sind IT-Sicherheit und Datenschutz überhaupt bezahlbar?

Um diese Frage zu beantworten, hat Hans-Georg Hunger im Rahmen eines Si-

Abb. 1 : Vorgehensweise zum Sicherheitscheck Datenschutz & IT-Sicherheit



cherheitschecks auf Basis des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie den einschlägigen Datenschutzgesetzgebungen die vorhandenen organisatorischen und technischen Sicherheitsstrukturen des Kreiskrankenhauses Greiz prüfen lassen. Zusätzliche technische und organisatorische Penetrationstests dienen zur Absicherung der oben aufgeführten Bereiche.

Die dabei aufgedeckten Defizite wurden priorisiert und in konkreten Handlungsmaßnahmen in enger und vertrauensvoller Zusammenarbeit mit der Datenschutzbeauftragten und dem IT-Bereich des Kreiskrankenhauses Greiz umgesetzt.

Die grundlegenden Sicherheitsvorkehrungen waren auch ohne großen Kostenaufwand möglich. Bereits mit ein paar einfachen Maßnahmen und Regeln, wie dem Erstellen einer internen Organisationsanweisung zum Datenschutz und dem Durchführen von Schulungen zu Datenschutz und IT-Sicherheit ließ sich der Sicherheitszustand im Klinikum wirksam erhöhen.



Uwe Günther, Geschäftsführender Gesellschafter der Sanovis GmbH:
 „Durchschnittlich 80 Prozent aller Sicherheitsbudgets fließen in Maßnahmen gegen Zugriffe von außen, gleichzeitig aber entstehen schätzungsweise 80 Prozent aller Schäden durch klinikinternen Fehlbenutzung oder Missbrauch.“

Maßnahmenkatalog* 1/5

UW-Mr.	Maßnahme	Anwenderkategorie	Priorität	Planungsbedarf
1	Wiederumsetzung von Zugriffsrechten	- Prüfung und Umsetzung möglicher Möglichkeiten, die Wiederumsetzung von Zugriffsrechten auf allen relevanten Systemen (einschließlich der Cloud) festlegen	hoch	unmittelbar
4	Widmung der Datenhaltung	- Festlegung der Widmung der Datenhaltung in allen Messdaten (z.B. Mitarbeitergespräche, Mitarbeiterkennzeichen, etc.)	mittel	mittelfristig
6	Speichern und Löschen von Daten	- Festlegung des Löschen und Löschrung möglicher Möglichkeiten (Speichern und Löschen von Mitarbeiterdaten)	gering	Langfristig
14	Organisationsanweisung Datenschutz	- Prüfung und Umsetzung von möglichen Möglichkeiten (einschließlich der Mitarbeiter, die Verantwortlichkeit, Integrität und Vertraulichkeit von sensiblen Daten gewährleisten)	hoch	In Arbeit
16	Schulung Datenschutz	- Organisationsanweisung von Mitarbeiterkategorien zum Datenschutz (einschließlich der Mitarbeiterkategorie)	hoch	unmittelbar
17	Arbeitsplatz PC	- Festlegung und Umsetzung möglicher Möglichkeiten, die Möglichkeiten zum Löschen von Daten (z.B. Mitarbeiterkennzeichen, etc.) festlegen	mittel	mittelfristig

Logo: KRANKENHAUS GREIZ, Sanovis GesundheitsCare

Abb. 2: Auszug aus dem Maßnahmenkatalog als Ergebnis des Sicherheitschecks

„Was waren die wesentlichen Erkenntnisse?“

„Für uns im Kreiskrankenhaus Greiz war es sehr wichtig alle Mitarbeiter bei der Identifikation und Bekämpfung der Gefährdungspotentiale mit einzubeziehen, denn nur ein gemeinsames Erarbeiten und Tragen der Maßnahmen stellt die lückenlose Verbesserung unserer Qualitäts- und Sicherheitsstandards sicher“, konstatiert Hans-Georg Hunger.

Dem kann Uwe Günther von der Sanovis GmbH nur zustimmen. „Es ist ganz wesentlich, dass ein Verbesserungsprozess aus der Klinik heraus selbst getrieben wird, der Berater hilft dabei die Ansatzpunkte zu identifizieren und deren Umsetzung zu begleiten. Die enge Zusammenarbeit mit dem Fachpersonal, der IT und dem Datenschutzbeauftragten war hier ebenso bedeutsam wie auch die Integration der IT-Hersteller und Lieferanten, welche ja einen Großteil der Systeme warten und betreiben. Allgemein kann man sagen, dass das Ablegen der Scheu vor Problemen und eine uneingeschränkte Offenheit unabdingbar sind, um etwaige Missstände zu beheben.“

www.hospital-greiz.de
www.sanovis.com

Die Joint Commission International Accreditation

Die Joint Commission on Accreditation of Healthcare Organizations (JCAHO) ist die älteste private, unabhängige und gemeinnützige Körperschaft zur Zertifizierung von Gesundheitseinrichtungen mit Sitz in Chicago. Der internationale Zertifizierungsprozess ist so konzipiert, dass er mit den gesundheitspolitischen, wirtschaftlichen, kulturellen und regionalen Gegebenheiten unterschiedlicher Länder zu vereinbaren ist.

Die 355 Standards, die nochmals in 1.007 einzelne Elemente aufgliedert sind, beinhalten zum Beispiel Richtlinien für die Behandlung, Untersuchung, Aufklärung und Sicherheit unserer Patienten sowie die Frage der Mitarbeiterqualifikation und Weiterbildung, der Unternehmensführung und Information in und außerhalb der Einrichtung. Im Ergebnis der Zertifizierung wurden die 355 geprüften Standards alle erfüllt.

www.jointcommission.org