AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe März 2016 | Seite 1

Datenschutzbeauftragte von Gesundheitseinrichtungen stehen täglich vor der Herausforderung, Sachverhalte in kürzester Zeit rechtlich und technisch zu bewerten sowie pragmatische Lösungsansätze zu entwickeln. Häufig ist hierfür der Rückgriff auf Fachliteratur unerlässlich. Auf aktuelle Themen kann diese allerdings nur selten zeitnah reagieren. Hier setzt unser neuer Fachinformationsdienst an. Mit diesem möchten wir Sie gerne in Zukunft kostenlos einmal im Monat über aktuelle rechtliche und technische Themen informieren, die wesentlichen Probleme dar- und Lösungsmöglichkeiten vorstellen. Die erste Ausgabe erhalten Sie heute in Papierform. Wir möchten unseren Fachinformationsdienst in Zukunft aber gerne elektronisch versenden und würden uns freuen, wenn Sie sich auf www.aok-verlag.info/ds-im-blick hierfür anmelden. Selbstverständlich völlig kostenlos und ohne Verpflichtungen.

Ihre AOK Verlags GmbH

INHALT

Vernichtung von Patientenakten

Aus Patientenakten wird Konfetti

Dr. Sebastian Ertel, Sven Venzke-Caprarese

Stellen Sie sich folgenden Sachverhalt vor: Sie nehmen als Zuschauer am Rosenmontagsumzug teil. Von einem Wagen wird in großen Mengen Konfetti geworfen. Sie fangen etwas davon auf und stellen beim genaueren Hinsehen fest, dass auf den Papierschnipseln noch Informationen wie Namen, Adressen, Telefonnummern sowie der Name eines Krankenhauses zu erkennen sind. Sie glauben, das gibt es nicht? So in etwa ist es beim diesjährigen Fasching in Dermbach (Thüringen) tatsächlich passiert. Die Papierschnipsel stammen, wie zwischenzeitlich ermittelt wurde, aus einem Thüringer Klinikum.

Ärztliche Schweigepflicht

Zwar befanden sich bei den Informationen wohl keine Aussagen über Diagnosen, Medikationen oder Behandlungsmaßnahmen. Wird aber erkennbar, dass die Daten aus einer medizinischen Behandlung stammen, kann bereits hieraus eine Verletzung der ärztlichen Schweigepflicht resultieren und der Straftatbestand des § 203 StGB erfüllt sein.

Ist das wirklich schon von der Schweigepflicht umfasst?

Bereits der Umstand, dass man sich in medizinische Behandlung begeben hat, unterliegt der ärztlichen Schweigepflicht. Brisanter wird es, wenn sich die medizinische Einrichtung nur auf ein Fachgebiet (z. B. Onkologisches oder Psychiatrisches Zentrum) spezialisiert hat. Dann können verhältnismäßig leicht Rückschlüsse auf den Gesundheitszustand gezogen werden.

Richtig Vernichten nach DIN 66399

Sind Dokumente der Vernichtung zuzuführen, ist die richtige Umsetzung anhand der DIN 66399 zu bewerten. Diese differenziert Daten nach Schutzklassen. Je sensibler die Daten sind, desto höher ist die

Schutzklasse zu wählen. Aufsichtsbehörden empfehlen für Behandlungsunterlagen (etwa Anamnese, Aufnahme- und Aufklärungsbögen, Befunde, Medikation, OP-Berichte) die Schutzklasse 3. Dies insbesondere deshalb, weil Geheimhaltungspflichten nach § 203 StGB zu beachten sind. Aus der Schutzklasse 3 leitet sich wiederum die Sicherheitsstufe ab. Die Sicherheitsstufe bestimmt die genauen Vorgaben, in welcher Partikelgröße bestimmte Medien vernichtet werden müssen. Aus der Schutzklasse 3 folgt nach der DIN 66399 z. B. eine Sicherheitsstufe von mindestens 4.

Mindestens Sicherheitsstufe 4?

Die Sicherheitsstufe 4 erlaubt eine Materialteilchenfläche von ≤ 160 mm². Eine Reproduktion der nach dieser Stufe verkleinerten Datenträger ist nur mit einem sehr hohen, nahezu unvertretbaren Zeitaufwand möglich.

3+1=4? Vorsicht!

Selbst wenn Gesundheitseinrichtungen in der Praxis einen Dienstleister mit der Vernichtung nach Sicherheitsstufe 4 beauftragen, ist an dieser Stelle äußerste Vorsicht geboten. Denn die DIN 66399 erlaubt einen Trick, den Dienstleister häufig nutzen: Weil durch Vermischen und Verpressen mit anderen Dokumenten die Reproduktion erschwert wird, sieht die DIN 66399 die Möglichkeit vor, Schreddergut mittels Vermischen und Verpressen der nächsthöheren Sicherheitsstufe zuzuordnen. Papierschnipsel der Sicherheitsstufe 3 können durch dieses Verfahren der Sicherheitsstufe 4 zugeordnet werden, obwohl sich an der Partikelgröße selbst nichts ändert. Zwar erkennt auch die DIN 66399 die Gefahr einer solchen Hochstufung. Sie macht diese daher auch von der Einwilligung des Auftraggebers abhängig. In der Praxis ist diese Einwilligung aber in vielen Verträgen der Dienstleister bereits vorformuliert und eine bewusste Entscheidung der Gesundheitseinrichtung liegt häufig gar nicht vor.

Besser nicht

Vergegenwärtigt man sich, was Sicherheitsstufe 3 bedeutet, muss jede Gesundheitseinrichtung für sich hinterfragen, ob sie einer entsprechenden Hochstufung durch Vermischen und Verpressen wirklich zustimmen will. Denn Sicherheitsstufe 3 erlaubt eine Partikelgröße von ≤ 320 mm², also beispielsweise auch 4 mm * 80 mm. Die einzelnen Schnipsel können somit doppelt so groß sein, wie bei der Sicherheitsstufe 4. Kann ausgeschlossen werden, dass sich auf den einzelnen Schnipseln noch sensible Informationen befinden?

Aus alten Akten wird ein neuer Rohstoff

Und noch etwas ist zu beachten: Das geschredderte Papier wird in der Praxis als Rohstoff und somit als Handelsware behandelt. Es wird frei auf dem Markt verkauft, um daraus z. B. Recyclingpapier herzustellen. Man muss sich bei der Wahl der Sicherheitsstufe und bei der Einwilligung zur Hochstufung daher immer ganz bewusst machen: Das geschredderte Papier unterliegt keinerlei Schutz mehr. Überspitzt könnte man sogar behaupten, dass

angemessen geschreddertes Papier sogar als Konfetti genutzt werden darf. Im eingangs erwähnten Fall kann allerdings davon ausgegangen werden, dass die Sicherheitsstufe der Vernichtung noch deutlich unter den Sicherheitsstufen 3 und 4 lag.

Audit

Der Vorfall in Thüringen kann für Datenschutzbeauftragte in Krankenhäusern durchaus zum Anlass genommen werden, um die eigene Aktenvernichtung noch einmal auf den Prüfstand zu stellen. Sofern Dienstleister mit der Vernichtung beauftragt sind, kann eine erneute Vertragsprüfung im Hinblick auf die vereinbarte Sicherheitsstufe und ggf. sogar ein Vor-Ort-Audit inklusive

Sichtung des Schreddergutes sinnvoll sein.
Ob und unter welchen Voraussetzungen die Einschaltung eines externen Dienstleisters zur Patientenaktenvernichtung überhaupt möglich ist, behandeln wir in der nächsten Ausgabe. In diesem Rahmen thematisieren wir auch, welche technischen und organisatorischen Maßnahmen zu beachten sind.

Vertiefungshinweis im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel C/11 (Datenträger sicher entsorgen)

Wenn Sie unseren Fachinformationsdienst in Zukunft regelmäßig erhalten möchten, melden Sie sich bitte unter www.aok-verlag.info/ds-im-blick für die elektronische Ausgabe an. Der Fachinformationsdienst ist und bleibt für Sie völlig kostenlos, begründet keinerlei Verpflichtungen und kann jederzeit abbestellt werden.

Krankenhäuser wegen Schadsoftware vom Netz

Welche Schutzmaßnahmen können ergriffen werden?

Sven Venzke-Caprarese, Dr. Sebastian Ertel

Die Medienberichterstattung über lahmgelegte Krankenhausnetzwerke wird in den letzten Wochen kaum an den IT-Abteilungen und Datenschutzbeauftragten von Gesundheitseinrichtungen vorbeigegangen sein. Allein im Februar 2016 wurde über mindestens vier deutsche Krankenhausgesellschaften in Neuss, Arnsberg, Kleve und Aichach berichtet, die von einer besonders aggressiven Schadsoftware betroffen waren: der Ransomware „Locky“.

Was ist Ransomware?

Bei Ransomware handelt es sich um eine Schadsoftware, die versucht, möglichst viele Dateien im betroffenen Netzwerk zu verschlüsseln und somit unmittelbar die Verfügbarkeit der Daten zu beeinträchtigen. Schlimmstenfalls sind die Daten auf unbestimmte Zeit verschlüsselt und praktisch verloren.

Die Schadsoftware beschränkt sich dabei nicht nur auf den Client eines einzelnen Anwenders, sondern befällt auch andere Speicher im Netzwerk, z. B. die auf einem Fileserver gespeicherten Dateien und Ordner. Einmal zum Zuge gekommen, informiert die Schadsoftware betroffene Nutzer über die Verschlüsselung und bietet eine Entschlüsselung gegen Zahlung von „Lösegeld“ an – z. B. mittels Bitcoins.

Wie kommt Schadsoftware ins Netzwerk?

Die Einfallstore für Schadsoftware generell und somit auch für Ransomware sind vielfältig. In den vorliegenden Fällen sollen z. B. präparierte Word- und Excel-Dokumente über E-Mail-Anhänge versandt worden sein und beim Öffnen der Dokumente eine Infektion verursacht haben. Hierbei wurden die Makrofunktionen der entsprechenden Office-Programme ausgenutzt, die eigentlich dazu dienen sollen, sich wiederholende Arbeitsabläufe in den jeweiligen Anwendungen zu automatisieren. Aber nicht nur E-Mail-Anhänge sind häufig Einfallstore. Auch schlecht gepatchte Webserver und Webapplikationen sind beliebte Angriffsziele und können sogar genutzt werden, um die Schadsoftware an Websitebesucher mit veralteten Browserver-

sionen weiter zu verteilen. Grundsätzlich gilt: Es wird versucht, jede Schwachstelle auszunutzen.

Wohl keine gezielten Angriffe auf Krankenhäuser

Derzeit ist davon auszugehen, dass die eingangs genannten Krankenhausgesellschaften nicht zielgerichtet angegriffen wurden, sondern von einer breit aufgestellten Angriffswelle erfasst wurden. Schätzungen gehen davon aus, dass im Februar 2016 zu Spitzenzeiten bis zu 5.000 Neuinfektionen pro Stunde zu verzeichnen waren. Grund genug, die bisherigen Schutzmaßnahmen gegen Schadsoftware noch einmal auf den Prüfstand zu stellen.

Schutzmaßnahmen

Bei der Betrachtung der Risiken zeigt sich schnell: Ein angemessener Schutz kann nur durch eine Vielzahl von Maßnahmen erreicht werden. Dabei kommen sowohl technische als auch organisatorische Maßnahmen in Betracht.

Patch- und Updatemanagement

Besonders wichtig ist ein funktionierendes Patch- und Updatemanagement. Denn viele Schwachstellen sind bereits bekannt und können durch vorhandene Patches und Updates geschlossen werden. Sofern diese jedoch nicht oder zu spät eingespielt werden, macht man es selbst breit angelegten und automatisierten Angriffswellen leicht, entsprechende Schadsoftware zu verteilen. Eine zentral gesteuerte Verteilung von Patches und Updates ist in der Praxis daher oftmals unerlässlich.

Virenscanner, Firewall, SMTP-Gateway

Auch der Einsatz von Virenscannern und Firewalls sowie eine Filterung auf Ebene des SMTP-Gateways stellen weitere Schutzmaßnahmen gegen die Infektion mit Schadsoftware dar. Insbesondere die Einstellungen des SMTP-Gateways sollten dabei ständig überprüft und ggf. der aktuellen Situation angepasst werden. Neben den üblicherweise zu filternden Dateiendungen könnte in der aktuellen Situation auch überprüft werden, ob die eingesetzten Filtertechniken eine gesonderte Behandlung von E-Mails erlauben, die Office-Dateien enthalten. In der aktuellen Situation kann es zudem sinnvoll sein, eine Ausdrucksfilterung z. B. anhand der E-Mail-Betreffzeile auf Ebene des SMTP-Gateways durchzuführen. Letztlich bleibt es aber immer ein Katz- und Mausspiel.

Makrofunktionen deaktivieren

Insgesamt sollte vor dem Hintergrund der aktuellen Geschehnisse die Notwendigkeit von Makrofunktionen von Office-Produkten kritisch hinterfragt und diese ggf. abgeschaltet werden. Je nach IT-Landschaft ist es z. B. möglich, Makrofunktionen über entsprechende Group Policies clientübergreifend zu sperren. Alternativ kann auch darauf geachtet werden, bereits im Rahmen der Standardinstallation die sicherheitskritischen Funktionen zu deaktivieren.

Einschränkung der Nutzerrechte

Nicht nur aus Gründen der Zugriffskontrolle ist eine Einschränkung der Nutzerrechte auf das erforderliche Mindestmaß sinnvoll. Dass normale Nutzer keine Admin-Rechte haben, gehört dabei zum Mindeststandard. Aber auch die Rechte auf Fileserverebene sollten möglichst eingeschränkt sein, um eine Ausweitung von Schadsoftware so gut es geht zu verhindern.

Netzsegmentierung

Insgesamt kann auch eine Segmentierung der Netze angebracht sein. Gerade in Krankenhausnetzwerken ist z. B. eine starke Trennung zwischen dem Gästenetz für Patienten, dem Verwaltungsnetz des Krankenhauses und dem Netzwerk, in dem sich medizinische Geräte und besonders sensible Anwendungen befinden, ratsam.

Mitarbeitersensibilisierung

Für den Fall, dass alle vorherigen technischen Sicherheitsmaßnahmen nicht greifen, ist eine Sensibilisierung der Mitarbeiter zwingend erforderlich. Neben Schulungen und regelmäßigen Awareness-Kampagnen bietet sich in der jetzigen Situation z. B. eine Rundmail bzw. eine Information der Mitarbeiter an, worauf zu achten ist. Hier sollte insbesondere darüber informiert werden, wie mit E-Mails aus unbekannten Quel-

len umgegangen werden soll und wer intern zu kontaktieren ist, wenn Mitarbeiter das Gefahrenpotential einer E-Mail nicht einschätzen können oder verdächtiges Verhalten der Clients feststellen.

Angemessenes Backup-Konzept

Zwar können all die genannten Maßnahmen das Risiko einer Infektion verringern. Hundertprozentige Sicherheit wird es jedoch nie geben. Im Fall der Fälle hilft letztlich nur noch ein Rückgriff auf vorhandene und nicht infizierte Backups. Dies setzt jedoch ein sorgfältig geplantes Backup-Konzept voraus. Dabei ist auch zu bedenken, dass die Backups so gespeichert werden müssen, dass sie bei einem Befall des Netzwerkes nicht gefährdet sind. Hier bietet sich z. B. die Speicherung auf externen Datenträgern, die nicht mit dem Netzwerk verbunden sind, an.

Notfall- und Recovery-Management

Das beste Backup-Konzept hilft nichts, wenn im Ernstfall eine Wiederherstellung, z. B. auf Grund fehlender Systemkonfigurationen, nicht möglich ist. Erforderlich ist insofern ein entsprechendes Notfall- und Recovery-Management. Zumindest sollte im Vorfeld einmal getestet worden sein, ob aus den vorhandenen Backups eine Wiederherstellung erfolgreich durchgeführt werden kann.

Fazit

In den eingangs erwähnten Fällen konnten die Daten laut Medienberichten aus vorhandenen Backups wiederhergestellt werden. Dennoch waren Ausfälle zu verzeichnen, die den Krankenhausbetrieb teilweise sehr einschränkten und z. B. die Aufnahme von neuen Patienten verhinderten. Schlimmeres konnte jedoch abgewendet werden.

Vertiefungshinweis im Handbuch DSiGW:

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel M/5.7.1 (Backup-Konzept), Kapitel M/5.7.3 (Update- und Patchmanagement), Kapitel M/5.7.4 (Virenschutzkonzept), Kapitel M/4.2.2 (Netzwerksegmentierung und Firewall)

Kurzinformationen

Neues zum IT-Sicherheitsgesetz

Bereits im Juli 2015 ist das IT-Sicherheitsgesetz in Kraft getreten. Dieses regelt künftig bestimmte Pflichten von Betreibern kritischer Infrastrukturen. Wer genau als Betreiber kritischer Infrastrukturen einzuordnen ist, war bislang unklar. Gewartet wurde insofern auf eine Rechtsverordnung (BSI-KritisV), die anhand von qualitativen und quantitativen Kriterien genau diese Fragen beantwortet. Für die ersten Bereiche (Sektoren) liegt seit Mitte Januar nun ein „Entwurf einer Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ vor. Dieser ist auch im Internet abrufbar (http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo.html). Der Sektor „Gesundheit“ wird in diesem Entwurf zwar noch nicht geregelt. Dies war aber auch nicht zu erwarten, da bereits vor einiger Zeit angekündigt wurde, die Sektoren Finanzen, Gesundheit und Transport/Verkehr in einem zweiten Korb Ende 2016 zu regeln. Dennoch lohnt sich auch für Betreiber von Gesundheitseinrichtungen ein Blick in den aktuellen Verordnungsentwurf: Von den im Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz genannten bis zu 2.000 Betreibern kritischer Infrastrukturen werden in dem aktuellen Entwurf für den ersten Korb schätzungsweise 650 Unternehmen angesprochen. Bleiben also für die Sektoren Finanzen, Gesundheit und Transport/Verkehr noch 1.350 Unternehmen übrig. Wie viele Krankenhäuser im zweiten Korb betroffen sein werden, ist nach wie vor unbestimmt. Klar zu sein scheint aber, dass nicht alle Krankenhäuser als kritische Infrastruktur bewertet werden. Wie die Abgrenzungskriterien im Sektor „Gesundheit“ gestaltet werden, ist derzeit offen. Als Kriterien in Betracht kommen könnten z. B. die Anzahl der versorgten Patienten bzw. die Bettenzahl oder die Spezialisierung auf bestimmte Gebiete. Genaueres wird jedoch voraussichtlich erst Ende 2016 bekannt sein. Nach Inkrafttreten der Verordnung stehen dann 6 Monate für die Einrichtung von Kontakt- und Meldestellen sowie 2 Jahre für die Implementierung eines Informationssicherheitsmanagements zur Verfügung.

Vertiefungshinweise im Handbuch DSiGW:

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel D/7 (IT-Sicherheitsgesetz), Kapitel M/7.2 (Aufbau eines ISMS)

EU-Datenschutz-Grundverordnung

Am 15.12.2015 haben sich die Vertreter des Europäischen Parlaments, der EU-Kommission und des Ministerrates im sogenannten Trilog auf die endgültige Fassung der EU-Datenschutz-Grundverordnung geeinigt. Diese soll durch europaweit unmittelbar geltende Regelungen einerseits den Betroffenen eine bessere Kontrolle über ihre personenbezogenen Daten geben und andererseits Unternehmen die Möglichkeit eröffnen, neue Technologien besser nutzen können. Auch für den Datenschutz im Gesundheitswesen wird die neue Verordnung umfangreiche Änderungen mit sich bringen. Zu beachten ist allerdings auch, dass insbesondere für die Verarbeitung von Gesundheitsdaten die Verordnung den Mitgliedstaaten einen relativ weiten Regelungsspielraum lässt, hier auch weiterhin nationale Regelungen zu den Bedingungen einer Datenverarbeitung zu erlassen.

Neben der Datenschutz-Grundverordnung wurde ebenfalls eine Einigung über die Richtlinie für den Datenschutz bei Polizei und Strafjustiz erzielt. Diese soll sicherstellen, dass die Daten von Opfern, Zeugen und Verdächtigen bei strafrechtlichen Ermittlungen oder im Strafverfahren in hinreichendem Maße geschützt sind.

Mit einer förmlichen Annahme von Verordnung und Richtlinie durch das Europäische Parlament und den Europäischen Rat wird im Frühjahr dieses Jahres gerechnet. Zwei Jahre später, voraussichtlich ab Mai 2018, gelten dann die neuen Vorschriften.

Vertiefungshinweise im Handbuch DSiGW:

Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel A/1.5 (Gesundheitsdatenschutz unter der EU-Datenschutz-Grundverordnung)

Handbuch „Datenschutz im Gesundheitswesen“

Neben diesem kostenlosen Fachinformationsdienst bieten wir ein umfangreiches Handbuch „Datenschutz im Gesundheitswesen“ an. In diesem finden Sie vertiefende Hinweise zu den Themen unseres Fachinformationsdienstes. Wir haben unseren Informationsdienst so gestaltet, dass die jeweiligen Themen für sich stehen und Sie keiner ergänzenden Lektüre bedürfen. Davon unabhängig leistet unser Fachbuch eine wichtige Hilfe für den Praxisalltag und stellt viele der im Fachinformationsdienst behandelten Themen nochmals umfassender und ausführlicher dar.

Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.300 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 74,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.

Newsletter-Anmeldung

Erhalten Sie einmal monatlich völlig kostenlos und unverbindlich wichtige Neuigkeiten und Fachinformationen zum Datenschutz im Gesundheitswesen.

Hier für den Newsletter anmelden:
www.aok-verlag.info/ds-im-blick