ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 01 2017

Der Datenschutzaudit

Von der Vorbereitung bis zur Durchführung

Akademie
Mit unseren Seminaren und Kongressen rund um Datenschutz, IT-Sicherheit sowie Spezialthemen

Praxismodell zur Einführung der DSGVO
Datenschutzkonforme Prozesse als Management-aufgabe – das Buch für Ihren Unternehmensalltag

Der sichere E-Mail-Versand
Er ist möglich, aber nicht praktikabel. Ist diese Ansicht berechtigt?

Akademie

Wir bilden Sie aus und fördern den Branchenaustausch für Datenschutz- und IT-Sicherheitsthemen. Hierzu nehmen wir als Referenten an einer Vielzahl von Kongressen und Messen teil und bieten darüber hinaus Seminare und Workshops an.

MESSE

Besuchen Sie uns auf Europas führender Veranstaltung für Gesundheits-IT

conhIT, Berlin 25.04.–27.04.17
NRW-Gemeinschaftsstand in Halle 1.2, Stand A-109

SEMINARREIHE

Wir bereiten Sie mit unseren Seminaren optimal auf die DSGVO vor!
4 Termine an 4 Standorten

Der medizinische Datenschutz im Lichte der DSGVO
Bis genau zum 24.05.2018 gilt es, die Anforderungen der ab 25.05.2018 geltenden DSGVO (Datenschutz-Grundverordnung) der EU umzusetzen. Die normative Anpassungsphase ist vergleichsweise kurz und die Ausgestaltung auf Bundes- und Landesebene bereits in vollem Gange. Um den Neuerungen und vor allem den Praxisanforderungen des Gesundheitswesens gerecht zu werden, veranstaltet die Agentur Esturias in Zusammenarbeit mit der DATATREE AG eine Seminarreihe an vier Standorten in ganz Deutschland.

Wie gut sind Sie vorbereitet?
Durch die aktuellen Gesetzesanpassungen kommt es regelmäßig zu weiteren Konkretisierungen. Für einen Großteil der Einrichtungen im Gesundheitswesen ergeben sich hierdurch viele Fragestellungen, was die konkrete, praxisnahe Umsetzung für das eigene Haus mit sich bringt. Die geplante Seminarreihe soll hierzu eine effiziente Hilfestellung bieten. Die Teilnehmerzahl pro Seminar ist auf maximal 35 Teilnehmer begrenzt.

MELDEN SIE SICH JETZT ZU IHREM WUNSCHTERMIN AN UNTER
https://www.esturias.de/seminarreihe-2017/

- **16.05.–17.05.2017 Hamburg**
- **07.06.–08.06.2017 München**
- **12.09.–13.09.2017 Düsseldorf**
- **28.11.–29.11.2017 Berlin**

Wichtiger Hinweis für die Esturias-Fortbildung:
- Für Fachanwälte IT- und Medizinrecht findet § 15 FAO mit 16,0 Vortragsstunden Anwendung.
- Für die ärztliche Fortbildung sind 8 Punkte zu erwarten.

KOSTENLOSE INFORMATIONSVERANSTALTUNG

Kennen Sie Ihr Datenschutzniveau? Testen Sie es jetzt! Unverbindlich, kostenlos und vertraulich!
Machen Sie jetzt mit uns einen Datenschutz-Erstcheck und lassen sich unverbindlich durch das ISDSG beraten.

Wir laden Sie herzlich
am 12.05.2017
um 17.00 Uhr
nach Dortmund ein.

Was Sie erwartet?
Unsere Veranstaltung startet mit einem Vortrag zum Thema „Sicherer Umgang mit Patientendaten".

Bei einem anschließenden Get-together haben Sie die Möglichkeit, mit unseren Beratern eine erste Sprechstunde wahrzunehmen und den Datenschutz-Erstcheck durchzuführen. Die Ergebnisse werden nach der Veranstaltung von unseren Experten ausgewertet und bei einem gemeinsamen Termin mit Ihnen besprochen.

Sie können den Termin nicht wahrnehmen?
Fragen Sie nach weiteren Terminen in Ihrer Nähe!

Für weitere Informationen zum Inhalt der Veranstaltung und Ihre Anmeldung steht Fabian Rüter unter **fabian.rueter@datatree.eu** zur Verfügung.

INDIVIDUELLE WORKSHOPS FÜR IHRE EINRICHTUNG

Selbstverständlich lassen wir Ihnen gerne ein individuelles Angebot für ein auf Ihre Bedürfnisse abgestimmtes Schulungskonzept zukommen.

Inhalt

Datenschutzaudits sind Großprojekte.

Bleibt verschlüsselte E-Mail-Kommunikation Zukunftsmusik?

ISDSG-Akademie 2

Das Team 4

Tipps & Fakten 6

Schwerpunkt

Der Datenschutzaudit – von der Vorbereitung bis zur Durchführung 8
Handlungssicherheit in fünf Phasen.

Voice

Interview mit Prof. Dr. Thomas Jäschke 12
Die Angleichung von Theorie und Praxis muss das Ziel sein.

Gastbeitrag

Herausforderungen im Krankenhaus 4.0 14
Ein Beitrag des Krankenhaus-Kompetenz-Centrums.

Verschlüsselte E-Mail-Kommunikation – möglich, aber nicht praktikabel? 16
Wie funktioniert sie, und worauf muss sich das Gesundheitswesen gefasst machen.

Patientendaten wirksam schützen 20
Cloud-Dienste als eine Möglichkeit.

Der Datenschutzbeauftragte

Erfüllung seiner Aufgaben trotz ständigen Zeitdrucks 22
Die Tätigkeit des Datenschutzbeauftragten ist auch Managementaufgabe.

Goldene Regeln

6. Goldene Regel: Bereiten Sie Datenschutzthemen praxisnah auf 23
Datenschutzthemen sollten zielgruppengerecht aufbereitet werden.

EDITORIAL

Liebe Leserinnen, liebe Leser,

2017 steht alles unter dem Tenor der Europäischen Datenschutz-Grundverordnung. Für uns Datenschützer bedeutet dies viel Vorbereitung. Zum einen unserer selbst, denn die neue Verordnung sowie das Anpassungsgesetz und weitere Regelungen der Bundesländer müssen verinnerlicht und aufbereitet werden. Zum anderen gilt es aber ebenfalls, schon frühzeitig in diesem Jahr mit der Anpassung von Prozessen in Ihrer Einrichtung zu beginnen.

Die gute Nachricht: Sie sind nicht allein! Scheuen Sie deshalb nicht den Austausch mit Fachkollegen und Profis für bestimmte Fachbereiche. Sie können davon nur profitieren. Für den gemeinsamen Austausch bietet die ExperSite Ihnen wieder einen breiten Überblick über verschiedenste Themen aus der Welt von Datenschutz und IT-Sicherheit.

Wir beschäftigen uns mit der E-Mail-Kommunikation und dem Alltag des Datenschutzbeauftragten. In unserem Schwerpunktthema zeigen wir auf, wie der Datenschutzaudit zu gestalten ist. Außerdem im Interview: Institutsleiter Prof. Dr. Thomas Jäschke über die Lücken zwischen Datenschutztheorie und Praxis.

N. Richard

Ihre Nina Richard
(Redaktionsleitung)

Das Team

„Fachexpertise, Professionalität und Praxisnähe“, so lässt sich das ISDSG-Team beschreiben. Aufgrund unserer Kernkompetenzen in den Bereichen IT, Datenschutz und Sicherheit sowie jahrelanger Erfahrung im Gesundheitswesen können wir Ihnen ein breites Spektrum an Unterstützung anbieten, das sich genau an Ihren Bedürfnissen orientiert.

Das ISDSG ist ein Dienstleistungsbereich der DATATREE AG und beschäftigt sich mit allen Fragen zum Thema IT-Sicherheit und Datenschutz mit Schwerpunkt auf den Akteuren des Gesundheitswesens. Wir unterstützen Kunden bei der Bewältigung von Datenschutz- und IT-Sicherheitsherausforderungen, die durch die fortschreitende Digitalisierung zunehmend auftreten.

Nina Richard
Marketing & Kommunikation

Als Verantwortliche für die Bereiche Marketing und Kommunikation ist sie Ansprechpartnerin für alle Fragen rund um das redaktionelle Angebot des ISDSG und der ExperSite.

✉ richard@isdsg.de

Jan Domnik
IT-Security

Zu seinen Kernaufgaben gehören die Durchführung und Koordination von Penetrationstests, die Auditierung von IT-Systemen und die Überprüfung von Sicherheitskonzepten.

✉ domnik@isdsg.de

Christine Thieme
Datenschutz

Sie ist die Spezialistin für Fragestellungen aus den Bereichen Direktmarketing und Marktforschung und unterstützt Sie bei der datenschutzkonformen Umsetzung Ihrer Projekte.

✉ thieme@isdsg.de

Magnus Welz
Datenschutz

Der Projektleiter begleitet Sie direkt vor Ort und koordiniert die umzusetzenden Maßnahmen. Zudem gehört die strategische Ebene der Projektarbeit zu seinen Schwerpunkten.

✉ welz@isdsg.de

Prof. Dr. Thomas Jäschke
Vorstand

Der Medizin-Wirtschaftsinformatiker ist Experte im Gesundheitssektor und Datenschutzbeauftragter für namhafte Einrichtungen im Gesundheitswesen. Als Institutsleiter ist er der Kopf des ISDSG-Teams.

✉ dsb@isdsg.de

Alexander Vogel
Datenschutz

Mit seinem fundierten Know-how im medizinischen Umfeld und dessen Informationssystemen begleitet er Ihre Prozesse und Abläufe praxisnah und zielorientiert.

✉ vogel@isdsg.de

Angelica Morina
Projektmanagement

Sie verfügt über ein breit gefächertes Leistungsspektrum und hat als Projekt- und Administrationsmanagerin Ihr Projekt in Bezug auf die Terminplanung und das Controlling fest im Blick.

✉ morina@isdsg.de

Thorben Beer
Datenschutz

Als Projektleiter kann er auf seine Erfahrung in mittelständischen IT-Beratungsunternehmen zurückblicken. Angepasst an Ihre Wünsche und individuelle Situation entwickelt er die für Sie richtigen Konzepte.

✉ beer@isdsg.de

Fabian W. Rüter
Vertrieb

Sie wünschen ein individuelles Angebot für die Themen Datenschutz oder IT-Sicherheit für Ihr Haus? Dann ist Fabian Rüter der richtige Ansprechpartner für Sie.

✉ rueter@isdsg.de

WUSSTEN SIE SCHON ...

dass die Bundesnetzagentur kürzlich verboten hat, die Puppe "My Friend Cayla" zu besitzen und zu kaufen? Diese wurde aufgrund des ungeschützten Zugriffs auf das Mikrofon via Bluetooth als verbotene Senderanlage eingestuft, um den Missbrauch der Puppe als als Spionagegerät zu verhindern.

Endlich gewusst wie: Das Umsetzungsmodell zur Einführung der EU-DSGVO

Jeder scheint sich aktuell mit ihr zu befassen: Die Europäische Datenschutz-Grundverordnung ist DAS Thema, mit dem sich gefühlt momentan jeder beschäftigt. So werden aktuelle Inhalte rezitiert, interpretiert und Annahmen für zukünftige Auslegungen in Bezug auf die praktische Umsetzung diskutiert. Was fehlt, ist allerdings eine konkrete Hilfestellung für die Einführung innerhalb des Unternehmens – ein Großprojekt, das eine Vielzahl von Prozessanpassungen mit sich bringt. Kontinuierliches und strukturiertes Datenschutzmanagement ist hierbei die Grundlage, um die kein Datenschützer herumkommt, wenn die DSGVO erfolgreich eingeführt werden soll.

Worum es NICHT geht:

- Es wird nicht die nächste Veröffentlichung sein, die sich mit der Umsetzung von Maßnahmen/ Anforderungen der DSGVO beschäftigt
- Keine juristische Ausarbeitung

Was Sie bekommen:

- Praktisches Umsetzungsmodell zur Einführung der DSGVO
- Detaillierte Beschreibung von Managementvorgehen von A wie (Bestands-)Aufnahme über Risikoanalyse und -bewertung bis Z wie (Optimierungs-)Zyklus, ausgerichtet an dem Großprojekt der Datenschutzgrundverordnung
- Übersichtliche Darstellung und Auffindbarkeit von relevanten Aspekten für Ihr Unternehmen
- Konkrete Hilfestellung und Handlungsempfehlungen für Ihr Unternehmen
- Checklisten

Titel:
Das Praxishandbuch zur DSGVO
Umsetzungsmodell und Maßnahmenkatalog zur praktischen Anpassung der bestehenden Datenschutzorganisation
(als E-Book erhältlich)

Herausgeber:	Prof. Dr. Thomas Jäschke
weitere Autoren:	Magnus Welz, Thorben Beer, Alexander Vogel, Nina Richard, Prof. Julius Reiter
Erscheinungsdatum:	Juni 2017
Preis:	19,99 Euro (Einführungspreis bis zum 31.08.2017)

Vorbestellungen sind ab sofort unter **www.datatree.eu/vorbestellung** möglich.

Awareness-Schulungen

Wie können Verantwortliche für den Datenschutz und die IT-Sicherheit die Mitarbeiter innerhalb der Einrichtung auf die Notwendigkeit dieser Themen hinweisen? Eine Möglichkeit bietet die Awareness-Schulung.

Die Vorteile:

- Sensibilisierung der Mitarbeiter
- Verringerung von Malware-Infektionen
- Verbesserung der Fehlerkultur

Grundsätzlich betrifft das Thema Awareness jeden Mitarbeiter, der an den Einrichtungsrechnern arbeitet, Zugriff auf das Internet hat und digitale Kommunikationswege wie E-Mail-Programme nutzt. Je nach Größe Ihrer Einrichtung kann es schwierig und unverhältnismäßig werden, jeden einzelnen Mitarbeiter persönlich schulen zu wollen. Es kann deshalb sinnvoll sein, die Schulung für ausgewählte Multiplikatoren anzubieten, die das Gelernte an Ihre Mitarbeiter weitergeben.

Auf den Inhalt kommt es an

Die meisten Ihrer Mitarbeiter werden wahrscheinlich schon bei dem Gedanken an eine IT-Sicherheits- oder Datenschutzschulung in einen meditativen Zustand verfallen. Versuchen Sie deshalb, nicht nur theoretische Aspekte wie Zahlen oder Gesetzestexte in die Agenda aufzunehmen, sondern holen Sie Ihre Mitarbeiter in ihrem Praxisalltag ab. Stellen Sie sich oder auch den Mitarbeitern deshalb ruhig im Vorfeld Fragen wie: Welche Probleme existieren im Alltag? Welche „Einfallstore" können Hacker in unserer Einrichtung nutzen? Existieren bereits Leitfäden für den Umgang mit dem Internet, E-Mails, mobilen Endgeräten?

Nachfolgende inhaltliche Punkte sollten bei der Konzeptionierung Ihrer Awareness-Schulung berücksichtigt werden:

Vorbereitung

Datenschutzbeauftragter/Informationssicherheitsbeauftragter und IT-Abteilung – Beispiele für Spam-Mails. Aber Achtung: Fangen Sie sich bei der Recherche nicht selbst einen Virus ein!

Grundlagen

- Sicherheitslücken
- Erfolgsquote von Hackerangriffen
- sichere Passwörter
- Gründe für Hackerangriffe
- Herausforderungen und Grenzen für den Schutz der Einrichtung
- Identifikation von Malware
- E-Mail-Anhänge
- Softwaredownload im Internet
- Durchführung von Angriffen
- Umgang mit schwierigen Passwörtern
- einrichtungsspezifischer Notfallplan (Kommunikationswege, Ansprechpartner, Verhaltensorientierung)

Nachbereitung

Stellen Sie übersichtliche Materialien zur Verfügung. Neben Ihrer Präsentation können das Beispiele mit konkreten Handlungsempfehlungen sein.

Der Datenschutzaudit – von der Vorbereitung bis zur Durchführung

Eine Begrifflichkeit und verschiedene Bedeutungen. Aber egal, ob es sich um einen gesetzlich geregelten Datenschutzaudit nach §9a BDSG oder einen internen Audit, in Form einer Prüfung von Datenschutzprozessen handelt – eines haben sie alle gemeinsam: Für zufriedenstellende Ergebnisse ist eine professionelle Vorbereitung, Durchführung und Nachbereitung unabdingbar.

Der Datenschutzaudit soll es Einrichtungen ermöglichen, ihr Datenschutzkonzept sowie die technischen Einrichtungen durch einen unabhängigen Dritten prüfen zu lassen (§ 9a BDSG) und so zur Verbesserung und Darstellung des Datenschutz- und Datensicherheitsniveaus beitragen. Viele Datenschutzbeauftragte fassen den Begriff eines Datenschutzaudits jedoch weiter und prüfen zusätzlich noch Prozesse innerhalb ihrer Einrichtungen hinsichtlich ihrer Datenschutzkonformität sowie der geforderten Umsetzung der technischen und organisatorischen Maßnahmen. Der Datenschutzauditor ist in diesem Fall der Datenschutzbeauftragte selbst. Der Datenschutzaudit – intern oder extern – ist ein komplexes und zeitintensives Projekt, das die Mitarbeit von allen Beteiligten verlangt.

Organisatorischer Ablauf eines Audits

Für einen Datenschutzaudit besteht keine generelle Pflicht. Jedoch kann er für Ihr Unternehmen Vorteile bringen. So kann der Audit, gerade wenn er zum ersten Mal durchgeführt wird, den aktuellen Ist-Stand und somit eine Übersicht für Sie als Datenschutzbeauftragter sein. Zudem verlangen gerade Krankenkassen von ihren Partnern meist ein Datenschutzaudit. Im Großen und Ganzen besteht ein Datenschutzaudit aus fünf Phasen:

1. **Phase:** organisatorische Vorbereitung
2. **Phase:** der Voraudit sowie ggf. Anpassungen
3. **Phase:** der (Haupt-)Audit
4. **Phase:** der Abschlussbericht
5. **Phase:** die Re-Auditierung

Phase 1: Organisatorische Vorbereitung
Das Projektmanagement obliegt in der Regel dem Datenschutzbeauftragten, der somit auch als hauptverantwortlicher Koordinator und Ansprechpartner innerhalb der Einrichtung gilt, um den Audit so optimal vorzubereiten. Bevor die inhaltliche Ausgestaltung für die Auditierung beginnt,

> *Bevor die inhaltliche Ausgestaltung für die Auditierung beginnt, gilt es, sich mit der Organisation des Projektes zu beschäftigen.*

gilt es, sich mit der Organisation des Projektes zu beschäftigen. Festgelegt werden sollte deshalb zum einen der konkrete Betrachtungsgegenstand, wobei klar definiert wird, welche Prozesse, Abteilungen oder Produkte einer Auditierung unterzogen werden, sowie eine Abgrenzung von nicht

auditierten Abteilungen und Prozessen. Das schafft neben der Dokumentationsfunktion die Möglichkeit, sich einen ersten Überblick über involvierte Personen zu verschaffen. In diesem Schritt sollte außerdem eine grobe Zieldefinition des Datenschutzaudits erfolgen. Die Ziele eines Audits können individuell festgelegt sein: von der Prüfung der technischen und organisatorischen Maßnahmen über die Sensibilisierung der Mitarbeiter bis zum allgemeinen Überblick über das Datenschutzniveau.

> *Die Ziele eines Audits können individuell festgelegt sein.*

Im nächsten Schritt sollte die Erstellung eines groben Zeitplans folgen und somit der Projektbeginn, das Projektende und – aufgegliedert in die fünf Auditphasen – die jeweilige Dauer der Teilphasen bestimmt werden. Hieraus kann anschließend der Projektplan mit entsprechenden Arbeitspaketen abgeleitet werden.

Im letzten Schritt dieser Phase werden die Ansprechpartner für die Prozesse bzw. der beteiligten Abteilungen dokumentiert.

Für einen internen Audit legen Sie die Dokumentation und die entsprechende Projektplanung der Geschäftsführung vor, sodass diese hiervon Kenntnis erlangt. Zusätzlich sollten aber bereits in diesem Projektschritt alle Beteiligten über den bevorstehenden Audit informiert werden. Lassen Sie Ihr Unternehmen durch einen externen Dienstleister auditieren, halten Sie die in Ihrer Dokumentation erarbeiteten Inhalte zusätzlich in dem geschlossenen Dienstleistungsvertrag fest.

Phase 2: Voraudit
Der Voraudit bildet die Vorbereitung für den (Haupt-)Audit. Falls noch nicht in der ersten Projektphase geschehen, sollte spätestens zu Beginn dieser Phase die Information über den bevorstehenden Audit an die beteiligten Personen erfolgen. Zudem gilt es, von ebendiesen eine Übersicht der Prozesse bzw. eine Auflistung der Abteilungstätigkeiten und weitere relevante Dokumente, wie z. B. Prozessbeschreibungen, anzufordern.

Es gilt, den Auditprozess regelmäßig zu reflektieren und zu wiederholen.

Diese Unterlagen bieten dem Projektverantwortlichen die Möglichkeit, den Datenschutzaudit im Detail vorzubereiten. Dieser sollte die vorliegenden Dokumente analysieren, indem Verfahren oder Prozesse studiert werden, offene und/oder unklare Punkte notiert und anschließend mit der jeweiligen Fachabteilung geklärt werden. Die erarbeiteten Informationen werden anschließend in den Projektplan implementiert. Im Sinne der Transparenz sollte auch dieser der Geschäftsführung vorgelegt werden. Nicht zu vergessen ist die lückenlose Dokumentation aller Aktivitäten. Dies vereinfacht zum einen den Überblick, zum anderen kann z. B. der Geschäftsführung jederzeit problemlos der aktuelle Ist-Stand mitgeteilt werden.

Prüfkriterien

Die Prüfkriterien sollten gesetzliche Normen und Standards erfüllen (egal, ob es sich um ein internes oder externes Audit handelt). Um vor bösen Überraschungen geschützt zu sein, ist es insbesondere bei externen Auditierungen empfehlenswert, vorab die Spezifikationen der Prüfkriterien zu erfragen – vor allem dann, wenn die Vergabe eines Siegels erfolgen soll.

Hinweis

Egal, ob Ihnen ein internes oder externes Audit bevorsteht, machen Sie sich mit den Ihnen vorliegenden Dokumenten vertraut, sodass Sie bei Fragen durch den Gutachter als kompetenter Ansprechpartner wahrgenommen werden können. Sie sollten deshalb nicht nur die Dokumente kennen, sondern sich ggf. fehlendes Wissen durch zusätzliche Literatur oder Befragung der Fachabteilungen aneignen.

Phase 3: (Haupt-)Audit
Für den Gutachter (intern: Datenschutzbeauftragter, extern: Dienstleister) bildet eine flächendeckende Vorbereitung durch die ihm vorliegenden Dokumente eine gute Grundlage und bietet weitreichende Informationen über die zu auditierenden Prozesse. Der Datenschutzbeauftragte hat auf dieser Basis die entsprechenden Abteilungen zu besichtigen, vorbereitete Rückfragen zu stellen und ggf. neu gewonnene Erkenntnisse zu hinterfragen. Hier gilt es, in der Dokumentation beschriebene Prozesse im alltäglichen Betrieb genauer zu analysieren, um den aktuellen Zustand im Bereich Datenschutz des Unternehmens darzustellen.

Alle hier gewonnenen Erkenntnisse dienen der Gutachten-/Berichtserstellung, in der alle gewonnenen Erkenntnisse niedergeschrieben werden und versucht wird, zu einem abschließenden Fazit oder Urteil in Bezug auf den Datenschutz für das Unternehmen zu kommen.

4. Phase: Abschlussbericht
Der Abschlussbericht bedeutet nicht etwa das Ende des Audits. Vielmehr sollte dieser genutzt werden, um Rückschlüsse auf

> *Der Abschlussbericht bedeutet nicht etwa das Ende des Audits.*

Schwachstellen und Gefährdungspunkte für den Datenschutz im Unternehmen zu ziehen. Des Weiteren kann der Bericht genutzt werden, um einen kurzen Bericht für die Mitarbeiter der Einrichtung auszuarbeiten und hier die Ergebnisse sowie Verbesserungspotenziale darzustellen. Zudem sollte ein konkreter Maßnahmenplan zur Umsetzung der sich hieraus ergebenden Aufgaben aufgestellt werden.

Nach dem Audit ist vor dem (Re-)Audit

Auch nachdem der Audit durchgeführt und Ihr Unternehmen bewertet wurde, kann man sich nicht einfach zurücklehnen, sondern muss die Maßnahmen, die sich aus dem Abschlussbericht ergeben, umsetzen. Außerdem heißt es jetzt: Nach dem Audit ist vor dem (Re-)Audit!

Für seriöse Auditierungs- und Zertifizierungsverfahren gilt, dass Sie sich alle zwei bis drei Jahre einem Re-Audit unterziehen müssen, um die gleichbleibende Qualität und somit die Nachhaltigkeit des Themas Datenschutz zu beweisen. ■

Alexander Vogel

Checkliste: Ihre Aufgaben bei einem Audit

Name	Beschreibung	Status
	Organisatorische Vorbereitung	
Planung	• Zieldefinition • Betrachtungsgegenstand • Abgrenzung aufstellen	☐
Projektplan	Erstellen Sie einen groben Zeitplan für den Ablauf des Voraudits und des Audits.	☐
Ansprechpartner	Benennen Sie Ansprechpartner für die einzelnen Abteilungen bzw. Prozesse, welche auditiert werden sollen.	☐
	Voraudit	
Anschreiben	Schreiben Sie die Ansprechpartner an und holen Sie die notwendigen Dokumentationen ein.	☐
Analyse	Analysieren Sie die bereitgestellten Unterlagen und passen Sie daraufhin die Zielsetzung sowie den Betrachtungsgegenstand für die einzelnen Abteilungen und Prozesse an.	☐
Vorbereitung	In diesem Schritt bereiten Sie sich auf das Auditieren der einzelnen Abteilungen und Prozesse vor. Beschäftigen Sie sich genauer mit diesen, um gezielter Fragen zu stellen.	☐
	Audit	
Audit	Begehen Sie die zu auditierenden Abteilungen und Prozesse und machen sich ein Bild von der alltäglichen Umsetzung. Vergleichen Sie die Dokumentation mit den tatsächlich gelebten Prozessen.	☐
Bericht erstellen	Nachdem Sie den Audit erfolgreich durchgeführt haben, müssen Sie Ihre gewonnenen Erkenntnisse in einem Bericht oder Gutachten niederschreiben.	☐
	Abschlussbericht/Nachbearbeitung	
Maßnahmen ableiten	Studieren Sie den Abschlussbericht genau und leiten Sie daraus Maßnahmen für Ihr Unternehmen ab.	☐
Umsetzung	Setzen Sie die abgeleiteten Maßnahmen systematisch um. So verbessern Sie den Datenschutz in Ihrem Unternehmen.	☐
Re-Audit	Bereiten Sie sich auf den nächsten Audit vor. Setzen Sie Maßnahmen um oder identifizieren Sie neue mögliche Schwachstellen. Motivieren Sie Ihre Mitarbeiter, die gezeigten Leistungen aus dem Audit beizubehalten.	☐

Exkurs Zertifizierung

Das Thema „Zertifizierung" wird als Qualitätsmerkmal auch für den Datenschutz immer beliebter. Der Markt von Anbietern wird in diesem Zusammenhang immer größer und unübersichtlicher – inklusive vieler schwarzer Schafe, denn die Vergabe von Siegeln im Rahmen einer Zertifizierung ist gesetzlich nicht geregelt. Die Bundesregierung wollte im Rahmen eines Datenschutzpakets im Jahr 2008 unter anderem ein Datenschutzauditgesetz auf den Weg bringen. Dieses sollte die wesentlichen Aspekte eines Datenschutzaudits regeln. Im Jahr 2009 wurde die Verabschiedung des Gesetzes gekippt, nachdem die Kritik an seinen Inhalten zu groß wurde.

Mit der DSGVO soll sich ab 2018 alles ändern. Zukünftig sollen die Aufsichtsbehörden offizielle Prüfstellen akkreditieren können, wodurch den Einrichtungen Transparenz gewährt werden und die Qualität der vergebenen Datenschutzsiegel vergleichbar gemacht werden soll. Die konkrete Umsetzung lässt allerdings noch auf sich warten.

Im Interview mit …

Prof. Dr. rer. medic. Thomas Jäschke
ist Vorstand der DATATREE AG und verantwortet hierdurch die Leitung des Instituts für Sicherheit und Datenschutz im Gesundheitswesen (ISDSG). Er ist seit über zehn Jahren als externer Datenschutzbeauftragter für Unternehmen , insbesondere Einrichtungen im Gesundheitswesen, tätig und unterstützt diese bei der Erstellung und Umsetzung von Datenschutz- und IT-Sicherheitskonzepten. Die Schwerpunkte seiner Professur an der FOM Hochschule für Oekonomie & Management sind IT-Security, Mobile Computing und Informationsmanagement. Seit Januar 2015 betreut Prof. Jäschke als wissenschaftlicher Leiter den Hochschulbereich IT-Management, der sowohl einen Bachelor- als auch einen Masterstudiengang beinhaltet.

Prof. Dr. Thomas Jäschke

Technisch hochkomplexe Geräte und Nutzer, die kaum mit der Weiterbildung hinterherkommen und oft das schwächste Glied in der Kette sind: Das Thema IT-Sicherheit wird fast an jeder Ecke von Experten aufgegriffen, die uns mitteilen, dass gehandelt werden muss. Wie das funktionieren soll, wissen allerdings die wenigsten. Nur mit einem ausreichenden Risiko- und IT-Sicherheitsmanagement kann es funktionieren.

ISDSG: Als Hochschulprofessor und Datenschutz- und IT-Sicherheitsexperte erleben Sie täglich sowohl die theoretische als auch die praktische Seite Ihrer Fachgebiete. Sehen Sie hier eine große Lücke zwischen Theorie und Praxis?
Tatsächlich ist festzustellen, dass Datenschutz und Informationssicherheit in der täglichen Praxis nicht immer ausreichend berücksichtigt werden. Gerade im Gesundheitswesen, beim Umgang mit besonders schützenswerten Daten, kommt es aber auf ein sorgfältiges Vorgehen im Sinne der rechtlichen Grundlagen an. Aus dem Alltag kann man sagen: Je kleiner die Organisation, desto weniger sensibel ist der Umgang mit diesen Daten. Manchmal kann dann auch von Gleichgültigkeit gesprochen werden. Natürlich gilt das nicht pauschal.

In vielen Fällen liegt die mangelnde Umsetzung im Datenschutz und in der IT-Sicherheit an fehlender Unterweisung der Mitarbeiter. Oft bekomme ich bei Schulungen Sachverhalte geschildert, die aus datenschutzrechtlicher Sicht sehr bedenklich sind. Von diesen Vorkommnissen weiß aber der Datenschutzbeauftragte selbst oft nichts, weil die Mitarbeiter keine Mitteilungen machen oder gar nicht wissen, dass ein solcher Vorfall intern gemeldet werden sollte.

Gerne wird auch behauptet, dass einer erkrankten Person Datenschutz ganz egal sei, solange ihr geholfen wird. Erläutert man allerdings, was es bedeutet, auf den Datenschutz zu verzichten, wird auf Nachfrage dann doch deutlich, dass nicht alle Personengruppen uneingeschränkt Kenntnis über die Patienteninformationen erhalten sollen, beispielsweise der Vorgesetzte.

Wäre eine Angleichung von Theorie und Praxis wünschenswert?
Aus meiner Sicht muss eine Angleichung von Theorie und Praxis immer das Ziel sein. Dabei ist aber nicht zu vergessen, dass die Anforderungen immer alltagsgerecht umgesetzt werden sollen, sodass die eigentliche Tätigkeit nicht behindert wird. Hier liegt es in der Verantwortung des Datenschutzbeauftragten, nicht als Störfaktor zu gelten, sondern unter Berücksichtigung der Verhältnismäßigkeit, Maßnahmen zu treffen, welche von den Mitarbeitern akzeptiert werden.

Für die meisten Fragestellungen und Prozesse gibt es gute Lösungsszenarien. In einigen anderen Fällen ist die Sachlage komplizierter und muss ggf. mit externen Fachleuten erörtert werden.

Überall ist mittlerweile die Rede vom selbstbestimmten Patienten und einer veränderten Servicekultur, gepaart mit Entwicklungen von E-Health-Anwendungen, die Behandlungen effizienter gestalten und Patienten ein immer besseres „Gefühl" vermitteln. Vor welche Herausforderungen stellt das den Datenschutz und die IT-Sicherheit?
Ein zentraler Gedanke ist, dass der Patient nicht nur Gegenstand der Behandlung sein will, sondern Teil davon. Durch die für alle zugänglichen Informationen und die zahlreichen Apps hat sich die Kommunikation zwischen den Leistungserbringern und den Patienten bereits verändert und wird es weiter tun. Dadurch steigen natürlich auch die Anforderungen an den Datenschutz, wenn es um personenbezogene Daten geht, und damit auch an die Maßnahmen der IT-Sicherheit.

Aktuell testet einer meiner Studierenden im Rahmen seiner Abschlussarbeit die Top-Ten-Apps aus dem Bereich Gesundheitswesen in Deutschland, Frankreich und Großbritannien auf Sicherheitslücken. Der aktuelle Zwischenstand der Ergebnisse zeigt schon jetzt, dass dort noch ein großer Optimierungsbedarf besteht. Das sollte uns zu denken geben und ein Ansporn für unsere weitere Arbeit sein.

„Wir sind im Bereich Datenschutz und IT-Sicherheit sehr gut aufgestellt." – Eine Aussage, die Sie bestimmt öfter mal von Krankenhausleitern zu hören bekommen. Aber mal Hand aufs Herz – wie sicher und gut geschützt sind unsere Krankenhäuser hier tatsächlich?
Vorweg, anders als bei größeren Arztpraxen oder auch anderen Unternehmen, die gesetzlich einen Datenschutzbeauftragten benötigen, aber keinen bestellt haben, findet man in jedem Krankenhaus einen Beauftragten für den Datenschutz. Auch die IT-Sicherheit ist nicht zuletzt durch die Vorfälle mit Verschlüsselungstrojanern in Krankenhäusern verstärkt in den Fokus gerückt. Leider bedeutet das nicht in allen Fällen, dass die Umsetzung auch den Anforderungen entspricht. Die Aufgaben sind vielfältig und es kommt aufgrund der unterschiedlichen Rollen, die eine Person erfüllen muss, oft zu Interessenskonflikten, entweder zeitlich oder inhaltlich. Gelegentlich erfährt man, dass der Personalleiter oder die Assistenz der Geschäftsführung mit den Aufgaben betraut wurde. In anderen Fällen mangelt es an der regelmäßigen Fortbildung des Datenschutzbeauftragten. Durch wenige Fragen wird meist schnell deutlich, ob in einem Krankenhaus der Datenschutz wirklich gelebt wird oder sein Dasein auf einem Stück Papier fristet.

Die Rolle des ISB (Informationssicherheitsbeauftragten) wird auch schon in vielen Häusern ins Leben gerufen. Einige Häuser erwarten durch das IT-Sicherheitsgesetz gesetzliche Verpflichtungen dazu, einen ISB zu bestellen. In Kliniken, in denen ein IT-versierter Datenschutzbeauftragter am Werk ist, kann es unter Berücksichtigung weiterer Rahmenbedingungen sogar sinnvoll sein, dass dieser auch die Rolle des ISB übernehmen kann.

Welchen Rat können Sie Klinikleitern und Datenschutzbeauftragten mitgeben?
Klinikleiter sollten sich regelmäßig über den Datenschutz im eigenen Haus unterrichten lassen und auf Übergabe entsprechender Datenschutzberichte bestehen, die auch im Falle eines Falles haftungsrechtlich einen Vorteil haben können. Datenschutzbeauftragte, vor allem diejenigen, die ihre Rolle nur in Teilzeit ausfüllen können, sollten darauf achten, sich regelmäßig um die Belange des Datenschutzes zu kümmern und diese auch von der Geschäftsführung einzufordern. Außerdem gilt es, sich bei Spezialfragen nicht unnötig zurückzuhalten. In einigen Fällen kann es sinnvoll sein, einen externen Experten hinzuzuziehen. ■

Interview: Nina Richard

Herausforderungen im Krankenhaus 4.0

Dass die digitale Welt auch ihre Schattenseiten hat, mussten vor Kurzem 180 Gäste eines Vier-Sterne-Hotels in Österreich erfahren, als Cyberkriminelle das gesamte IT-System des Hotels blockierten. Die elektronischen Schlüsselkarten wurden sofort unwirksam und die Gäste konnten ihre Zimmer nicht mehr verlassen bzw. betreten. Erst gegen eine Zahlung von 1.500 Euro in Bitcoin entsperrten die Hacker das System.

Für eine Klinik in Los Angeles war die Freischaltung ihrer IT-Systeme etwas teurer: 15.000 Euro. In Großbritannien wurden bereits 30 Prozent der staatlichen Krankenhausorganisationen (NHS Trusts) Opfer eines Ransomware-Angriffs. Auch deutsche Krankenhäuser, Stadtverwaltungen und Unternehmen machten schon ihre kostspieligen Erfahrungen mit Trojanern wie Locky, TeslaCrypt, Nemucod und Cerber. Im Jahr 2016 war eine Steigerung dieser erpresserischen Attacken um 80 % zu beobachten.

Manfred Kindler
ist seit 1986 öffentlich bestellter und vereidigter Sachverständiger für Medizinprodukte, seit 1998 Consultant für Qualitäts- und Risikomanagement (ISO 17000 Familie) und seit 2015 im Präsidium des KKC e. V.

Erfolgreiche Angriffe finden Nachahmer

Insbesondere Malware im Netzwerk oder auf PCs ohne Virenschutz, oft von E-Mails mit Anhängen transportiert, öffnet den Attacken zunächst unbemerkt gefährliche Eingangstore. Eine besondere Herausforderung für die Cybersecurity stellt das Internet der Dinge (Internet of Things – IoT) dar. Schlecht vernetzte Geräte wie Webcams, Drucker, Router, Videorecorder, aber auch Baby-Monitore wurden im Oktober 2016 vom Botnetz Mirai zusammengeschaltet und für eine Attacke auf den Internet-Knotenpunkt Dyn missbraucht, sodass weltweit Dienste wie Twitter, Reddit, Netflix, Spotify oder Papypal für Stunden ausfielen. Einen Monat später legte Mirai fast eine Million Telekom-Router lahm. Mittlerweile ist der Quellcode für Mirai im Netz veröffentlicht, eine Fundgrube für Nachahmer. So ist es nicht verwunderlich, dass Ende November 2016 ein Mirai-Botnetz mit 400.000 IoT-Geräten im Internet zur Miete angeboten wurde. Die Anzahl der im Internet vernetzten Geräte steigt exponentiell: von 5 Mrd. im Jahr 2010 auf 16 Mrd. im Jahr 2015 und für 2020 werden 200 Mrd. IoT-Komponenten erwartet. Lebensbedrohlich werden Cyberangriffe, wenn sie im Krankenhaus die vernetzte Medizintechnik treffen. So informierte kürzlich ein US-Medizingerätehersteller die Kunden seiner Insulinpumpe über eine Sicherheitslücke, nämlich die unverschlüsselte Funkverbindung zwischen der Pumpe und deren Fernbedienung, über welche Hacker die Dosierung leicht umprogrammieren könnten.

> *Eine besondere Herausforderung für die Cybersecurity stellt das Internet der Dinge (Internet of Things – IoT) dar.*

Fehlende IT-Strategien

Aufgrund schwerer Zwischenfälle warnt der Medizintechnik-IT-Sachverständige Armin Gärtner seit Jahren vor Sicherheitsdefiziten in den MT-Netzwerken. Computertomografen und Magnetresonanztomografen konnten keine Bilder mehr abspeichern, weil ein Hersteller in einem WLAN seine IP-Datenpakete als Voice-over-IP gekennzeichnet hatte, um diese Datenpakete mit Priorität über das Netzwerk zu schicken. Auf einer Intensivstation wurden wegen Konflikten von IP-Adressen Alarme nicht weitergeleitet. Netzwerke waren durch zeitgleiche Downloads von Windows-Updates oder Live-Streaming von Bildern aus einem Schlaflabor ausgefallen bzw. überlastet. Kürzlich begutachtete Gärtner den Fall eines Broadcast-Sturms in einem IT-Netzwerk, der für mehrere Stunden zum Ausfall aller bettseitigen Überwachungsmonitore und deren Datentransfer zur Zentrale führte.

> *Die überwiegende Mehrzahl der Kliniken besitzt keine dezidierte IT-Strategie.*

Medizinproduktegesetz, Betreiberverordnung, IT-Sicherheitsgesetz und Risikomanagement nach DIN EN 80001-1 sollen die Digitalisierung im „Krankenhaus 4.0" sicherer machen. Doch wie sieht die Realität aus? Die überwiegende Mehrzahl der Kliniken besitzt keine dezidierte IT-Strategie. Die deutschen Krankenhäuser sind daher den digitalen Bedrohungen überwiegend hilflos ausgeliefert, trotz umfangreicher Kampagnen zum Thema Cybersecurity. Bei einer Befragung der Führungskräfte erklärten sich nach eigener Einschätzung gerade einmal 11% von ihnen als „sehr fit" in Sachen Digitalisierung. Unzureichende Investitionen in moderne IT-Systeme, wenig nutzerfreundliche Applikationen, fehlende Standards durch Insellösungen und Partikularinteressen einzelner Berufsgruppen lassen IT-Projekte häufig scheitern. Vor den Türen warten bereits die disruptiven Innovationen des Cognitive Computing und der künstlichen Intelligenz. (IBM Dr. Watson lässt grüßen, zumindest schon im Universitätsklinikum Marburg der Rhön-Klinikum AG.) ■

Manfred Kindler (Präsident des KKC)

Zum KKC

Vor 20 Jahren fanden sich auf der MEDICA Düsseldorf vier technische Fachverbände des Gesundheitswesens zu einem Gemeinschaftsstand zusammen. Das Krankenhaus-Kommunikations-Centrum (KKC) bietet seit 2001 eine unabhängige neutrale Plattform mit direktem Zugang zu politischen Entscheidern und baut mit seinem Metanetzwerk durch Round Tables, Streitgespräche, Expertenrunden und gemeinsame Tagungen interdisziplinäre Brücken für Akteure in den Bereichen Verwaltung, Medizintechnik und IT, Technikmanagement, Labormedizin, Pflegemanagement, Einkauf und Logistik, Controlling, Aus- und Fortbildung.

Als Premium-Partner des KKC engagiert sich das ISDSG zunehmend für die Erweiterung von Datenschutz- und IT-Sicherheitsstrategien im vernetzten Gesundheitswesen. ISDSG-Vorstand Prof. Dr. Thomas Jäschke ist hier in der Expertengruppe IT-Sicherheit sowie im wissenschaftlichen Beirat des KKC tätig.

Verschlüsselte E-Mail-Kommunikation – möglich, aber nicht praktikabel?

„Schick mir die Patientenfotos doch mal eben per E-Mail, damit ich draufschauen kann." Alltag in deutschen Kliniken. Haben auch Sie heute schon eine E-Mail mit personenbezogenen Daten bekommen? Im beruflichen Alltag verlassen wir uns darauf, dass die IT-Abteilung schon für die Sicherheit der digitalen Kommunikation gesorgt hat. Doch auch bei etablierten Kommunikationsmedien darf man nicht ohne Weiteres davon ausgehen, dass die Inhalte vertraulich bleiben.

E-Mail, das ist klar, ist zeit- und ressourcensparend. Viele von uns nutzen ihre Inbox sogar als persönlichen Assistenten und To-do-Liste in einem (wie sich das auf unsere Arbeitsorganisation auswirkt, ist eine andere Frage).

Doch eins ist die herkömmliche E-Mail nicht: vertraulich. Das gilt auch für die sogenannte transportverschlüsselte E-Mail (TLS) – eine solche liegt immer noch auf verschiedenen Stationen ihres Wegs unverschlüsselt und fremdem Zugriff gegenüber ungeschützt vor. Erst die Ende-zu-Ende-verschlüsselte E-Mail ist tatsächlich vertraulich, wie beispielsweise auch die gematik in ihrem letzten Whitepaper zur Sicherheit der Telematik-Infrastruktur[1] angemerkt hat.

> *Erst die Ende-zu-Ende-verschlüsselte E-Mail ist tatsächlich vertraulich.*

Bereits seit Anfang der 1990er gibt es Software, die es dem E-Mail-Nutzer ermöglicht, Ende-zu-Ende-verschlüsselte Mails zu verschicken. Doch warum hat sich diese Verschlüsselung bis heute nicht durchgesetzt?

Entwicklung unserer heutigen Verschlüsselungsmechanismen

E-Mail wurde in den 1960er-Jahren entwickelt, als nur eine Handvoll Einrichtungen an den ersten Vorläufer des Internets angebunden waren. Die Einzigen, die einem der Mainframe-Rechner nah genug kommen durften, um eine E-Mail zu verschicken, waren eine Handvoll Wissenschaftler. Diese hinterließen sich in ihren Benutzerkonten gelegentlich digitale Notizzettel – E-Mail. Niemand sah daher anfangs die Notwendigkeit, E-Mail gegen unbefugtes Mitlesen oder Fälschung zu sichern. Dementsprechend sucht man die Verschlüsselung oder andere Sicherheitsmechanismen im ursprünglichen E-Mail-Protokoll vergeblich.

Hier kommt PGP ins Spiel: „Pretty Good Privacy" („Ziemlich gute Privatsphäre"), das 1991 von Phil Zimmermann entwickelte Protokoll zur E-Mail-Verschlüsselung. Wenige Jahre später erblickte das zweite der heute verwendeten Verschlüsselungsprotokolle die Welt: S/MIME.

Die Besonderheit von PGP und S/MIME ist das Schlüsselpaar aus öffentlichem und privatem Schlüssel. Wenn Sie über einen unsicheren Kanal– beispielsweise das Internet – verschlüsselt kommunizieren wollen, stellt sich die Frage: Wie können Sie den geheimen Schlüssel an Ihren Gesprächspartner übermitteln, ohne dass ihn jemand abfängt? PGP und S/MIME umgehen dieses Problem, denn der öffentliche Schlüssel darf ruhig abgefangen werden – Sie können ihn sogar aktiv öffentlich machen, beispielsweise auf Ihrer Homepage oder einem Schlüsselserver. Der öffentliche Schlüssel ist nämlich nur dazu in der Lage, eine Nachricht zu verschlüsseln, nicht zu entschlüsseln. Zu Letzterem brauchen Sie den privaten Schlüssel, den Sie tatsächlich sorgfältig geheim halten müssen. Mit ihm können Sie sowohl Dokumente entschlüsseln (siehe Abbildung 1) als auch signieren.

> *Die Qualität eines S/MIME-Zertifikats hängt davon ab, wie zuverlässig Sie sich gegenüber der Zertifikatsstelle ausgewiesen haben.*

Die Qualität eines S/MIME-Zertifikats hängt davon ab, wie zuverlässig Sie sich gegenüber der Zertifikatsstelle ausgewiesen haben: Während es für ein Klasse-1-Zertifikat ausreicht, dass Ihre E-Mail-Adresse gültig ist und Sie Zugriff auf sie haben, müssen Sie sich für ein Klasse-3-Zertifikat persönlich bei der Zertifizierungsstelle ausweisen.

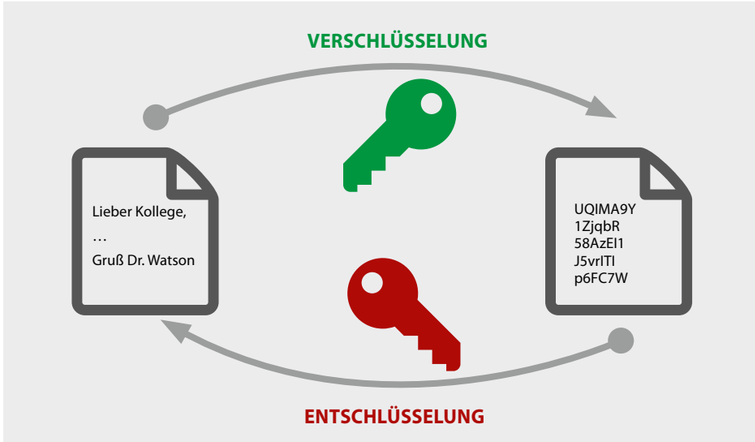


Abb. 1: Asymmetrische Verschlüsselung

So weit, so gut. Wie lässt sich aber verhindern, dass jemand Ihrem Gesprächspartner einen öffentlichen Schlüssel unterschiebt, der gar nicht Ihrer ist? Dazu dient das sogenannte Zertifikat, ein elektronisches Dokument, in dem festgehalten ist, dass ein bestimmter Schlüssel zu einer bestimmten E-Mail-Adresse und bestimmten Personalien gehört.

Können Sie sich ausweisen? Zertifikate & Signaturen

Bei PGP signieren Ihre persönlich bekannten Gesprächspartner Ihr Zertifikat und bestätigen damit gegenüber Dritten, dass Ihr Schlüssel zu Ihnen gehört und Sie tatsächlich Sie sind. S/MIME löst diese Aufgabe hierarchischer: Die Zertifikate werden von Zertifikatsstellen ausgestellt und signiert, deren Zertifikate ihrerseits wieder von übergeordneten Stellen signiert werden.

Dieses hierarchische Konzept wurde auch vom deutschen Gesetzgeber übernommen: Um mit einem Zertifikat eine qualifizierte elektronische Signatur (QES) zu ermöglichen, wie sie beispielsweise im Rahmen der Telematik-Infrastruktur im Gesundheitswesen notwendig wird, muss der Zertifikatsinhaber (beispielsweise der Inhaber des Heilberufsausweises) sich gegenüber der Zertifikatsstelle (beispielsweise mediSign) persönlich ausweisen – und einige weitere technische Anforderungen erfüllen.

> *Unverschlüsselte E-Mail ist, das hat sich herumgesprochen, nicht als vertrauliche Kommunikationsform zu betrachten.*

Unverschlüsselte E-Mail ist, das hat sich herumgesprochen, nicht als vertrauliche Kommunikationsform zu betrachten. Dies ist vor allem dort relevant, wo Berufsgeheimnisse (§ 203 StGB) bewahrt werden müssen und besonders schützenswerte Daten kursieren – beispielsweise im Gesundheitswesen oder zwischen Juristen und ihren Klienten.

Interessanterweise wird mittlerweile auch von der gematik darauf hingewiesen, dass die reine Transportverschlüsselung von E-Mails nicht vertraulich ist und mit dem § 203 StGB (Verletzung von Berufsgeheimnissen) in Konflikt steht. Das sah der Gesetzgeber vor nicht allzu langer Zeit noch anders: Der auf seine Initiative hin eingerichtete, lediglich transportverschlüsselte Dienst De-Mail wurde zunächst als ebenso vertraulich wie die Briefpost erklärt. Erst 2015 wurde hier mit der Einführung von PGP die Option zur tatsächlich vertraulichen Kommunikation geschaffen.

Warum also werden immer noch vertrauliche Patientendaten unverschlüsselt hin- und hergeschickt?

Unkompliziert oder sicher kommunizieren?

Zunächst einmal erfordert die Einrichtung einer Verschlüsselung einen gewissen Erstaufwand: Sie müssen sich für Ihren E-Mail-Client ein zusätzliches Plugin installieren (beispielsweise Enigmail[2] für Mozilla Thunderbird), dann müssen Sie ein Schlüsselpaar generieren, einen sicheren Aufbewahrungsort für Ihren privaten Schlüssel wählen und schließlich Ihren öffentlichen Schlüssel mit Ihren Kommunikationspartnern austauschen.

Hier gleich der nächste Haken: Wer von Ihren Kommunikationspartnern verschlüsselt schon mit dem gleichen Verfahren wie Sie? Wenn Sie Pech haben, niemand. An dieser

> *Wer von Ihren Kommunikationspartnern verschlüsselt schon mit dem gleichen Verfahren wie Sie? Wenn Sie Pech haben, niemand.*

Stelle kommt die kritische Masse ins Spiel: Da PGP- oder S/MIME-Nutzer nur untereinander verschlüsselt kommunizieren können, also eine Art soziales Netzwerk darstellen, wird die Teilnahme erst dann attraktiv, wenn bereits genug Personen im Netzwerk sind. Die ersten Nutzer müssen also ungewöhnlich viel Motivation aufweisen, um das Verfahren trotz geringer Teilnehmerzahlen zu adoptieren.

Warum nicht mal eine Cryptoparty besuchen! Hier treffen sich Datenschutzinteressierte.

Auch wenn Sie die Installation geschafft haben und als PGP- oder S/MIME-Nutzer gut untereinander vernetzt sind, ist die Anwendung auch weiterhin nicht ohne Tücken: Zunächst einmal steht und fällt die Sicherheit des Systems mit der Sicherheit des privaten Schlüssels – wenn Ihr privater Schlüssel in fremde Hände gelangt, ist Ihre gesamte zurückliegende Kommunikation sowie Ihre zukünftige (bis Sie den Diebstahl des Schlüssels bemerken) nicht mehr vertraulich. (Aus diesem Grund wird der Schlüssel zusätzlich mit einem Passwort geschützt. Die Sicherheit hängt also wiederum von der Passwortstärke ab.)

Die theoretische Sicherheit des eingesetzten Verschlüsselungsverfahrens – also die Tatsache, dass die Verschlüsselung ohne den privaten Schlüssel mit heutiger Rechenpower nicht in realistischer Zeit zu knacken ist – ist gleichzeitig ein Nachteil: Wenn Sie den privaten Schlüssel verlieren, können Sie Ihre verschlüsselte Kommunikation selbst nicht mehr lesen.

Der private Schlüssel muss zudem auf jedem Gerät liegen, auf dem Sie verschlüsselte Nachrichten lesen möchten. Berühmt wurde die Antwort von PGP-Erfinder Zimmermann auf eine verschlüsselte Mail: „I cannot decrypt this on my iPhone. Please send this to me again, in plaintext."

Da der Nutzer – wie so oft in Fragen der Datensicherheit – eine Abwägung zwischen Sicherheit und Komfort treffen muss, verleiten diese Eigenheiten von PGP und S/MIME dazu, Abkürzungen zu nehmen, die die Sicherheit kompromittieren: Schlüssel auf leicht zugänglichen Datenträgern zu speichern, unverschlüsselte Sicherheitskopien von Nachrichten anzufertigen und – wie Phil Zimmermann oben – die Verschlüsselung schließlich ganz zu umgehen.

Vertrauliche Daten müssen verschlüsselt werden

Trotzdem gilt für die Public-Key-Verschlüsselung wahrscheinlich sinngemäß, was Churchill einst über die Demokratie sagte: Sie ist die schlechteste Methode der Verschlüsselung – außer allen anderen Methoden. Aktuell wird beispielsweise auch die sichere Kommunikation unter Leistungserbringern (KOM-LE) in der Telematik-Infrastruktur auf der asymmetrischen E-Mail-Verschlüsselung basieren (Whitepaper der gematik von September 2016). Die Zertifikate werden zentral signiert, also wie im S/MIME-Verfahren. Zertifikate und Schlüssel liegen auf dem Heilberufeausweis und auch ein Verzeichnis mit auf Echtheit geprüften Adressen ist vorgesehen.

Dass die KOM-LE im Gesundheitswesen noch nicht flächendeckend ausgerollt ist, ist keine Rechtfertigung, um personenbezogene Daten unverschlüsselt zu verschicken. Das hat man auch in anderen Branchen erkannt: Die Bundesnotarkammer beispielsweise stellt schon lange digitale Zertifikate aus. Zur S/MIME-Verschlüsselung mit diesen Zertifikaten empfiehlt sie die kommerzielle Software SecSigner. In vielen Privatunternehmen wird stattdessen weiterhin auf Microsofts E-Mail-Client Outlook gesetzt, der

> *Wer aber nicht gerade damit rechnet, Ziel eines Geheimdienstes zu sein, fährt auch mit einer kommerziellen Verschlüsselungssoftware sicher besser als ganz ohne Verschlüsselung.*

die S/MIME-Funktionalität bereits eingebaut hat. Anhänger von Open-Source-Software weisen zwar darauf hin, dass kommerzielle Software, deren Quellcode nicht öffentlich einsehbar ist, tendenziell unsicherer ist als Open-Source-Software, weil Hintertüren unerkannt bleiben. Wer aber nicht gerade damit rechnet, Ziel eines Geheimdienstes zu sein, fährt auch mit einer kommerziellen Verschlüsselungssoftware sicher besser als ganz ohne Verschlüsselung.

Wenn die eigene Organisation noch keine Software zur Verschlüsselung etabliert hat, ist für die ersten Schritte zur Verschlüsselung der eigenen Mails die Lösung Mozilla Thunderbird mit dem Plugin Enigmail (beides kostenlos und Open Source) empfehlenswert. Enigmail verwendet OpenPGP – man benötigt also kein Zertifikat einer zentralen Stelle, sondern kann sofort mit dem verschlüsselten Mailen loslegen. Sobald man einige Kommunikationspartner hat, die ebenfalls PGP verwenden, kann man gegenseitig seine Zertifikate signieren und in diesem „Web of Trust" das Vertrauensniveau erhöhen.

Sie kennen niemanden, der seine Mails verschlüsselt, möchten aber trotzdem damit anfangen? Warum nicht mal eine Cryptoparty besuchen! Hier treffen sich Datenschutzinteressierte, erklären sich gegenseitig Software und tauschen ihre Schlüssel aus. Eine Liste von lokalen Veranstaltungen finden Sie unter **https://www.cryptoparty.in.** ■

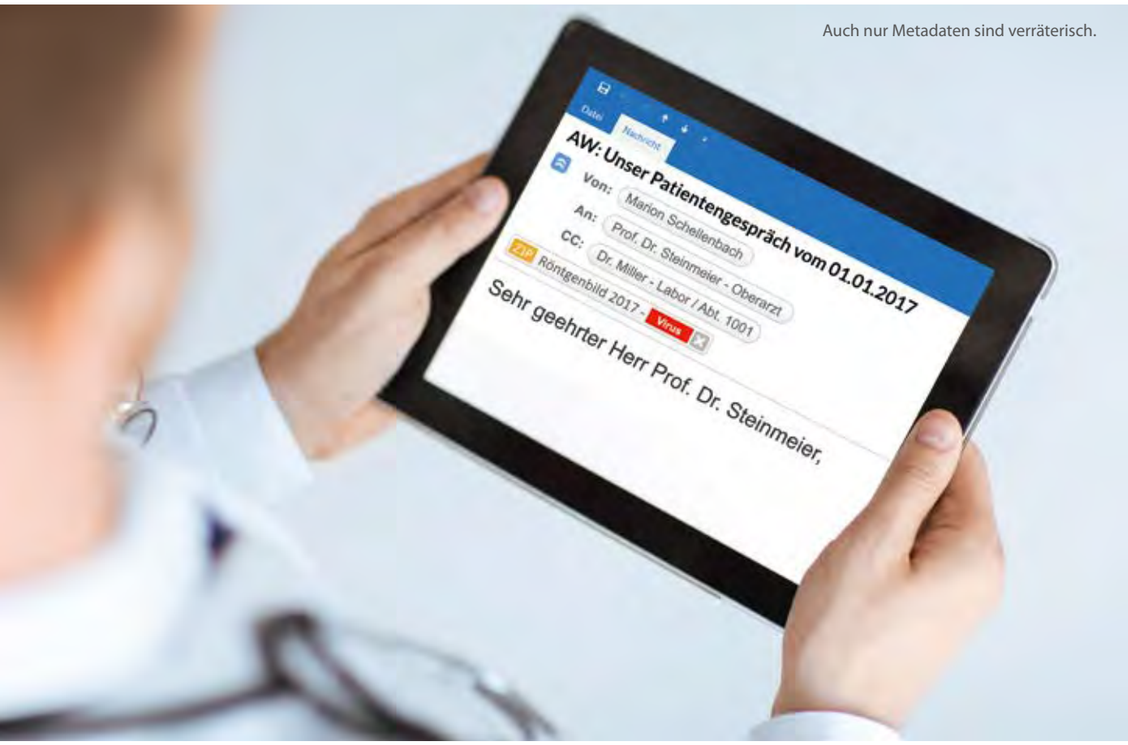
Dr. Christina Czeschik

Dr. Christina Czeschik (www.serapion.de) ist Ärztin für Medizinische Informatik und Fachautorin für E-Health, Datenschutz und IT-Sicherheit. Wie Sie einfach sicher digital kommunizieren, erklären sie und ihre Co-Autoren im Buch „Gut gerüstet gegen Überwachung im Web" (Wiley-VCH, 2015).

Weiterführende Informationen:

1 https://www.gematik.de/cms/media/info-materialpresse/gematik_whitepaper_web_Stand_270916.pdf
2 https://www.enigmail.net/

Anzeige



Auch nur Metadaten sind verräterisch.

Patientendaten wirksam schützen

Patientendaten sind Gold wert – und das ruft verstärkt Hacker auf den Plan. Statt für Kreditkarteninformationen interessieren sich Cyberkriminelle in den letzten Monaten verstärkt für Patienten- und Behandlungsdaten, die sich auf dem Schwarzmarkt gewinnbringend verkaufen lassen. Wie können Ärzte, Krankenhäuser und Apotheken ihre Patienten schützen?

Claudia Seidl ist Autorin, Journalistin und Bloggerin. Spezialisiert auf Privatsphäre im Internet schreibt sie unter www.idgard.de/privacyblog/ über die neuesten Entwicklungen im Bereich Datenschutz und IT-Sicherheit.

Hacker machen vor nichts Halt, auch nicht vor Krankenhäusern. Das musste im vergangenen Jahr bereits das Lukaskrankenhaus in Neuss am eigenen Leib erfahren. Damals hatten Hacker das System mithilfe einer E-Mail mit einem Trojaner infiziert und anschließend versucht, mehrere Tausend Euro von der Klinik zu erpressen.[1]

> *In den letzten Monaten sind Patienten- und Behandlungsdaten verstärkt in den Fokus von Hackern gerückt.*

Patientendaten im Fadenkreuz

Zwar war der Plan der Hacker nicht aufgegangen, die Software hatte aber trotzdem Schaden in Millionenhöhe verursacht und die gesamte Krankenhaus-IT für mehrere Tage lahmgelegt.

Nun haben Cyberkriminelle eine neue Masche gefunden: In den letzten Monaten sind Patienten- und Behandlungsdaten verstärkt in den Fokus von Hackern gerückt.[2] Millionen von gestohlenen Datensätzen – hauptsächlich, aber nicht ausschließlich von US-Krankenhäusern – stehen bereits auf den einschlägigen Handelsplattformen im Darknet zum Verkauf.

Wertvoller als Kreditkartendaten

Für Hacker ist dabei besonders interessant, dass solche Daten sehr viel länger verwertbar sind als beispielsweise Kreditkarteninformationen. Bemerkt der Kunde den Verlust oder Missbrauch seiner Kreditkarte, kann er diese sperren lassen, eventuell angefallene Buchungen stornieren und eine neue Karte anfordern. Patientendaten hingegen können nicht storniert oder gesperrt werden. Die Hacker können diese für Erpressungen nutzen oder glaubwürdige Rechnungen von Praxen, Krankenhäusern oder Apotheken fälschen. Auch Identitätsdiebstahl ist möglich – und das sogar noch Jahre nachdem die Daten entwendet wurden. Kein Wunder also, dass die gestohlenen Datensätze auf dem Schwarzmarkt zum Teil stolze Preise von bis zu 50 US-Dollar pro Akte erzielen. In der Regel werden aber gleich ganze Datenbanken zum Verkauf angeboten.

> *Patientendaten können, im Gegensatz zu Kreditkarten, nicht storniert oder gesperrt werden.*

„Die Technologie in vielen Praxen und Krankenhäusern ist veraltet und oft überhaupt nicht auf Onlinekommunikation ausgelegt", sagt Prof. Dr. Thomas Jäschke, Datenschutzbeauftragter und Leiter des Institutes für Sicherheit und Datenschutz im Gesundheitswesen (ISDSG). „Angreifer haben dort leichtes Spiel." Daher sei es wichtig, eine technische Lösung zu finden, mit der Patientendaten wirksam vor unbefugten Zugriffen geschützt werden können.

Schutz nach TCDP

Eine gute Möglichkeit, sensible Daten verlässlich zu schützen, sind Cloud-Angebote, die nach dem Anforderungskatalog des „Trusted Cloud Datenschutz Profils" (TCDP)[3] zertifiziert sind und eine möglichst hohe Schutzklasse (3 oder 3+) besitzen. Die Schutzklassen ergeben sich aus den technischen und organisatorischen Maßnahmen, die der Dienst der Daten und für die IT-Sicherheit einsetzt. Schutzklassen erleichtern den Cloud-Nutzern grundsätzlich die Wahl und unterstützen sie dabei, die von Datenschutzgesetzen geforderten Kontrollpflichten zu ersetzen. Mit Diensten wie beispielsweise iDGARD von Uniscon lassen sich vertrauliche Daten nicht nur verschlüsselt speichern, sondern auch sicher übermitteln. Sowohl die Daten als auch die Metadaten sind dabei nicht nur zuverlässig vor Angreifern geschützt, sondern können auch nicht vom Cloud-Anbieter selbst eingesehen werden. Darüber hinaus hat der Besitzer der Daten – also beispielsweise der untersuchende Arzt – auch volle Kontrolle darüber, wer wie oft auf welche Daten zugreifen kann und welche Zugriffsrechte er hat.

„Dazu kommt, dass iDGARD nicht nur Compliance sichert, sondern auch komfortabel und benutzerfreundlich ist", sagt Dr. Hubert Jäger, CTO bei Uniscon. „Die gespeicherten Daten können vom Nutzer jederzeit und von überall eingesehen werden. Auf diese Weise können Krankenhäuser, Versicherungen oder der Medizinische Dienst der Krankenversicherung (MDK) auch große Daten sicher und ohne Zeitverlust untereinander austauschen. Und das Beste: Dazu muss niemand neue Software installieren, der gesamte Zugriff erfolgt verschlüsselt über den Browser."

Mit iDGARD.hospital 20 und iDGARD.hospital 40 bietet Uniscon gleich zwei Pakete speziell für Krankenhäuer an. Informieren Sie sich jetzt unter **www.idgard.de.** ■

Claudia Seidl

Weiterführende Informationen:

1 https://www.idgard.de/privacyblog/ransomware-sabotiert-krankenhaeuser
2 https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf
3 https://www.idgard.de/service/downloads datenschutzzertifizierung-von-cloud-diensten/

Der Datenschutzbeauftragte – Erfüllung der Aufgaben trotz ständigen Zeitdrucks

Der Datenschutzbeauftragte berät die Geschäftsführung, Abteilungsleiter und Mitarbeiter der Unternehmen im Gesundheitswesen in allen relevanten Datenschutz- und Datensicherheitsthemen und wahrt gleichzeitig das Recht auf informationelle Selbstbestimmung von Patienten und Bürgern. Trotz dieser enorm wichtigen Aufgaben wird die Tätigkeit des Datenschutzbeauftragten häufig nebenher und unter Zeitdruck ausgeführt.

Trotz der fehlenden formalen Entscheidungsbefugnisse eines Datenschutzbeauftragten im Gesundheitswesen obliegt diesem eine hohe Verantwortung.

Aufgaben eines Datenschutzbeauftragten

Er muss nicht nur die gesetzlichen Vorschriften zum Datenschutz kennen, sondern ebenso Know-how im Bereich der Informationstechnologie mitbringen, Kontrollen bzgl. der Einhaltung der Datenschutzgesetze in sämtlichen Abteilungen eines Krankenhauses durchführen und sein Wissen an alle Mitarbeiter eines Krankenhauses weitergeben, sobald personenbezogene Daten von Patienten verarbeitet werden.

Nur so kann ein geschützter Umgang mit Patientendaten gewährleistet werden. Neben diesen Tätigkeiten ist der DSB außerdem für die Prüfung und Einhaltung von Auftragsdatenverarbeitungen (§11 BDSG) verantwortlich, führt Vorabkontrollen bei Verfahren automatisierter Datenverarbeitungen durch und muss außerdem noch Patienten Auskunft geben, wenn diese Fragen bzgl. der Verarbeitung ihrer Daten haben. Dies sind nur einige Beispiele für die vielschichtige Tätigkeit eines DSB. Aber wie können diese Aufgaben erledigt werden, wenn der DSB „nur" neben seiner Hauptposition bestellt ist?

Gelingt eine erfolgreiche Aufgabenerfüllung?

Prinzipiell lässt sich nicht genau sagen, wie viel Zeit ein DSB für die Erfüllung seiner Aufgaben benötigt. Das hängt von einigen betrieblichen und persönlichen Faktoren ab. Zum einen spielen die Größe des Krankenhauses und die Mitarbeiteranzahl eine Rolle. Zum anderen hängt der Zeitaufwand von der Anzahl der genutzten Datenverarbeitungsanlagen innerhalb eines Krankenhauses und von der Wissenslage eines DSB ab.

> *Prinzipiell lässt sich nicht genau sagen, wie viel Zeit ein DSB für die Erfüllung seiner Aufgaben benötigt.*

Damit ein DSB seine Aufgaben adäquat erfüllen kann, ist die Geschäftsleitung innerhalb eines Krankenhauses dafür verantwortlich, geeignete Mittel zur Bewältigung der Aufgaben zur Verfügung zu stellen. Zu nennen sind in diesem Kontext z. B. Weiterbildungsmöglichkeiten, geeignete Büroräume und ausreichend Sachmittel wie Fachliteratur. Sind die zu erledigenden Aufgaben z. B. zu groß oder fachlich komplex, sollte die Krankenhausleitung dem DSB Hilfspersonal bzw. externe Dienstleister zur Unterstützung zur Verfügung stellen. Gerade bei DSBs, die in Teilzeit bestellt sind, wird ohne ausreichende Unterstützung die Erledigung der Aufgaben im Datenschutzbereich nur schwer zu bewerkstelligen sein.

Wie kann Zeitdruck vermieden werden?

Die Erledigung der Aufgaben eines DSB ohne Zeitdruck hängt auch davon ab, ob dieser rechtzeitig in IT-Projekte, z. B. Implementierung einer neuen Datenverarbeitungsanlage, eingebunden wird. Eine frühzeitige Information und Unterrichtung des DSB über neue Anlagen ist gesetzlich vorgeschrieben (§ 4g Abs. 1 S. 1. Nr. 1 BDSG) und hilft, ein geeignetes Zeitmanagement aufzubauen. Auch eine Freistellung des DSB von sonstigen Aufgaben kann zu weniger Zeitdruck führen.

Fazit

Ein DSB innerhalb eines Krankenhauses oder anderer Institutionen im Gesundheitswesen hat eine verantwortungsvolle Position – er sorgt dafür, dass die äußerst sensiblen Patientendaten vor unberechtigtem Zugriff oder Verlust geschützt werden. Hierfür sind dem DSB ausreichend Ressourcen zur Verfügung zu stellen, damit die Aufgaben trotz knapper Zeit erfüllt werden können. ■

Susann Zorbach

6. Goldene Regel: Bereiten Sie Datenschutzthemen praxisnah auf

Für viele Mitarbeiter und Kollegen im Unternehmen ist das Thema Datenschutz eine trockene und langweilige Angelegenheit. Zudem hört man immer wieder: „Der Datenschutz verkompliziert und verhindert neue Projekte und Innovationen." Eines der größten Probleme für viele Mitarbeiter ist jedoch die Umsetzung im Alltag. Dabei fehlt es häufig nur an Beispielen dafür, wie Maßnahmen konkret in den beruflichen Alltag eingegliedert werden können.

Im Alltag begegnen dem Datenschutzbeauftragten viele Situationen, in denen Mitarbeiter und Kollegen Hilfestellung zum Thema Datenschutz erhalten wollen. Hierbei besteht die Schwierigkeit, die Themen so aufzubereiten, dass diese einfach im Alltag umgesetzt werden können.

Beispiel 1: Datenschutzschulungen

Ein gutes Beispiel für eine praxisnahe Gestaltung des Datenschutzes stellen die Schulungen dar. Im Bundesdatenschutzgesetz wird hierzu festgelegt, dass alle Personen, die mit der Verarbeitung von personenbezogenen Daten beauftragt sind, auf alle Gesetze, die den Datenschutz betreffen, hingewiesen werden müssen. Erfahrungsgemäß reicht es jedoch nicht, wenn den Mitarbeitern bei der Datenschutzschulung nur die relevanten Gesetzestexte vorgelesen werden. Fast alle Schulungsanwesenden werden innerhalb der ersten paar Minuten ihr Desinteresse bekunden.

Interaktive Gestaltung

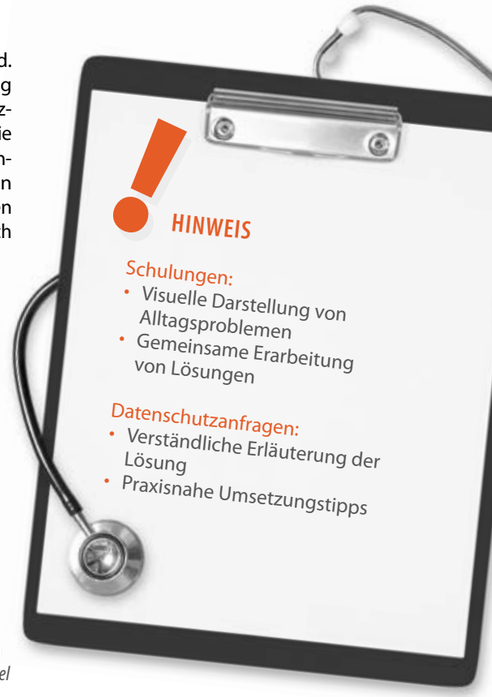
Die Problematik hierbei ist, dass für die meisten Schulungsteilnehmer die Gesetzestexte und Anforderungen zu abstrakt sind. Sie benötigen konkrete und für den Alltag schnell umsetzbare Tipps zum datenschutzkonformen Umgang mit Patientendaten. Die visuelle Darstellung und die mit den Teilnehmern gemeinsam entwickelten Lösungen von Problemen aus dem Praxisalltag erzielen größere Aufmerksamkeit und führen dadurch auch zu einem höheren Wissensgewinn.

Beispiel 2: Datenschutzanfragen

Eine weitere Gelegenheit, bei der Datenschutzthemen praxisnah aufgearbeitet werden können, sind Datenschutzanfragen von Mitarbeitern des Unternehmens. Die Mitarbeiter kommen mit alltäglichen Problemen zum Datenschutzbeauftragten und wollen wissen, wie sie diese in Bezug auf den Datenschutz anzugehen haben.

Hierbei sind keine ausführlichen Gesetzesinterpretationen notwendig. Es reicht, dem Anfragenden einfache Tipps oder Maßnahmen an die Hand zugeben. ■

Alexander Vogel



Impressum

ExperSite Ausgabe 01 2017 | ISSN-Print 2364-5636 | ISSN-Internet 2364-5644 | **Herausgeber:** ISDSG – Ein Dienstleistungsbereich der DATATREE AG Datatree AG, Heubesstraße 10, 40597 Düsseldorf, T +49 211 93190-700, F +49 211 93190-799, office@datatree.eu, www.datatree.eu | **Sitz der Gesellschaft:** Düsseldorf | **Registergericht:** Amtsgericht Düsseldorf | **Registernummer:** HRB 66132 | **Umsatzsteuer-Identifikationsnummer:** DE 279402614 | **Vorstand:** Prof. Dr. Thomas Jäschke | **Vorsitzender des Aufsichtsrates:** Prof. Dr. Julius Reiter | **Inhaltlich Verantwortlicher gemäß** § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV: Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Richard | **Editorial Design u. Umsetzung:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titel: Shutterstock, joker1991; S. 2: Shutterstock, Trueffelpix ; S. 3: Falko Wübbecke, Dortmund; Shutterstock, Panchenko Vladimir | TippaPatt; S. 4/5: Falko Wübbecke, Dortmund; S. 7: Shutterstock, Spectral-Design; S. 8 : Shutterstock, Panchenko Vladimir; S. 11: Falko Wübbecke, Dortmund; S. 14: Shutterstock, Kzenon | Kindler; S. 16: Shutterstock, Melpomene; S. 18: Shutterstock, Matej Kastelic; S. 19: Czeschik; S. 20: Shutterstock, Syda Productions | Seidl; S. 22: iShutterstock, frank_peters; S. 23: shutterstock, Maksim Kabakou | Tyler Olson; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke

"You don't have to bother checking the patients on this side. I already looked at their charts and they're doing just fine."

Wir bedanken uns für die inhaltlichen Beiträge bei:

Dr. Christina Czeschik, serapion.org
Manfred Kindler, Krankenhaus-Kompetenz-Centrum
Claudia Seidl, Uniscon GmbH

Die nächste Ausgabe erscheint im September 2017

Schwerpunkt:
Datenschutz – eine Managementaufgabe