ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 02 2017

Datenschutz-managementsystem

Perfekt vorbereitet auf die EU-DSGVO

Ransomware von der Stange

Schützen Sie sich effizient vor Hackerangriffen

Akademie
Wir bilden Sie aus: Rund um die Themen Datenschutz, Informationssicherheit oder EU-DSGVO

Datenschutz
Sinnvolles Projektmanagement: So bauen Sie Ihr Datenschutzmanagementsystem auf

Informationssicherheit
Mit Initiative für mehr Sicherheit: Gut gewappnet gegen Hackerangriffe

Akademie

Wir bilden Sie aus und fördern den Branchenaustausch für Datenschutz- und Informationssicherheit. Sie sind auf der Suche nach den richtigen Seminaren und Workshops? Dann werfen Sie einen Blick auf unsere Auswahl an Seminaren, Workshops und Tagungen.

MESSEN

Treffen Sie uns persönlich auf der Medica 2017 vom 13.-16. November in Düsseldorf.

SEMINARE

Datenschutzgrundverordnung

Der medizinische Datenschutz im Lichte der EU-GVO

Bereit für den Endspurt
Bis genau zum 24.5.2018 gilt es, die Anforderungen der ab 25.5.2018 geltenden Datenschutzgrundverordnung (EU-DSGVO) 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.

Wie gut sind Deutschlands Gesundheitseinrichtungen 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 UNSEREM NÄCHSTEN TERMIN AN.

https://www.esturias.de/seminarreihe-2017/

- **28.11.–29.11.2017 Berlin**

Kompaktseminar Datenschutz

Der Einstieg in den Beruf des Datenschutzbeauftragten ist nicht immer leicht. Neben einer Vielzahl von gesetzlichen Anforderungen sind auch persönliche und branchenspezifische Kenntnisse mitzubringen. Mit unserem Kompaktkurs Datenschutz erlangen Sie alle Grundlagen, die Sie als Datenschutzbeauftragter benötigen, um erfolgreich in Ihren beruflichen Alltag zu starten. An vier Terminen erhalten Sie das notwendige Expertenwissen, um als gesetzlich geforderter Datenschutzbeauftragter unternehmensintern wie -extern agieren zu können. Neben juristischen und informationstechnologischen Kenntnissen steht dabei u. a. der Ausbau kommunikativer sowie betriebswirtschaftlicher Kompetenzen auf dem Lehrplan.

DER NÄCHSTE KURS FINDET IN DÜSSELDORF AN FOLGENDEN TERMINEN STATT:

- **Freitag, 22.09.2017**
- **Freitag, 29.09.2017**
- **Freitag, 06.10.2017**
- **Freitag, 13.10.2017**

Der Kurs findet jeweils von 09.00 bis 16.30 Uhr statt und schließt mit einer schriftlichen Prüfung ab.

Datenschutzbeauftragter (IOM)

Im Rahmen des zehntägigen berufsbegleitenden Zertifikatslehrgangs „Datenschutzbeauftragte/-r“ erlangen die Teilnehmer das notwendige Expertenwissen, um als gesetzlich geforderte Datenschutzbeauftragte unternehmensintern wie -extern agieren zu können. Neben juristischen und informationstechnologischen Kenntnissen steht dabei u. a. der Ausbau kommunikativer sowie betriebswirtschaftlicher Kompetenzen auf dem Lehrplan.

DER NÄCHSTE KURS FINDET IM JANUAR 2018 IN ESSEN STATT.

INDIVIDUELLE WORKSHOPS FÜR IHRE EINRICHTUNG

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

- Auftragsverarbeitung
- EU-DSGVO
- Mitarbeiterschulungen
- Datenschutz
- Informationssicherheit

Inhalt

Bereiten Sie sich frühzeitig auf die Anforderungen des Gesetzgebers vor.

ISDSG-Akademie 2

Das Team 4

Neuigkeiten 6

Schwerpunkt 8
Das Datenschutzmanagementsystem
Mit diesen Schritten erfüllen Sie die gesetzlichen Anforderungen

Voice
Im Interview mit Dr. Christian Stoffers 12
Hand in Hand: So funktioniert die Kommunikation zwischen DSB und Marketer.
Nutzen Sie die Synergien mit Ihrer Marketingabteilung? 12
Profitieren Sie von Ihren gemeinsamen Schnittstellen

Der Datenschutzbeauftragte
So bauen Sie einen Draht zu Ihren Kollegen auf 14
Gestalten Sie Datenschutzthemen lebendig

Goldene Regeln
7. Goldene Regel: Verpflichten Sie Ihre Mitarbeiter 15

Informationssicherheit
Mehr Initiative für Ihre Informationssicherheit 17
Werden Sie aktiv für Ihre Einrichtung
Erpressungstrojaner von der Stange 18
Simplizität von Angriffen

Gastbeitrag
IT-Sicherheit: „Investieren Sie richtig?“ 20
Experten melden sich zu Wort

Der Informationssicherheitsbeauftragte
Aufgaben und Kerntätigkeiten des Informationssicherheitsbeauftragten 22
So gestaltet sich das Berufsbild

EDITORIAL

Liebe Leserinnen, liebe Leser,

lassen Sie uns enger zusammenrücken – so wie es auch die Bereiche Datenschutz und Informationssicherheit zunehmend tun.

Technische Entwicklungen, gepaart mit rechtlichen Anforderungen und Management-Know-how, machen die Betrachtung von Teilbereichen immer schwieriger und unvereinbar. Auch die ExperSite wird sich zukünftig gleichermaßen beiden Themenbereichen widmen.

Praxisnah und von internen sowie externen Expertenstimmen geprägt bereiten wir aktuelle Themen für Sie auf und unterstützen Sie bei der Vorbereitung auf die Datenschutzgrundverordnung oder das Informationssicherheitsgesetz.

Aber auch Tipps, wie Sie ihre Arbeit bekannt machen und sie in Ihre Einrichtung integrieren, sind, wie gewohnt, fester Bestandteil dieser Ausgabe.

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.

TEAM ORGANISATIONSENTWICKLUNG

Datenschutz und Informationssicherheit sind mehr als das Erfüllen von gesetzlichen Anforderungen. Gemeinsam mit Ihnen machen wir Ihre Themen greifbar und erlebbar.

Prof. Dr. Thomas Jäschke Vorstand und Datenschutzbeauftragter:
„Gelebter Datenschutz und Informationssicherheit sind Erfolgsgaranten für die digitale Welt.“

Nina Richard:
„Datenschutz und IT-Sicherheit sind langweilig? Ich zeig´ Ihnen das Gegenteil!"

Fabian Rüter:
„Datenschutz und Informationssicherheit sind Investitionen in die Zukunft“

Angelica Morina:
„Ihre Zufriedenheit ist mein oberstes Gebot."

TEAM DATENSCHUTZ

Unsere Expertise ermöglicht es uns, alle Aspekte des Datenschutzes für Ihre Einrichtung anwendbar umzusetzen.

Alexander Vogel
„Wir unterstützen bei der Bildung einer umfassenden Vertrauensbasis zwischen Arzt und Patient.“

Susann Zorbach:
„Datenschutz trotz IT und Cloud? Natürlich!“

Bettina Sandrock:
„Datenschutz heißt auch mal dran bleiben und einen Kampf gegen Windmühlen führen …“

Christine Thieme
„Datenschutz bedeutet Individualität und Detailarbeit – denn keine Anfrage ist wie die andere.“

Thorben Beer:
„Nur gelebter Datenschutz ist effektiver Datenschutz!“

Magnus Welz:
„Die Anforderungen an den Datenschutz im Gesundheitswesen sind hoch – das bedeutet aber nicht, dass sie im Alltag nicht praxisnah integrierbar sind.“

TEAM IT-SICHERHEIT

Vom Informationssicherheitsbeauftragten über Social Engineering bis hin zu Penetrationstests optimieren wir Ihre IT-Sicherheit.

Jan Domnik
„Für einige Menschen bedeutet Informationssicherheit, das Management von der groben Fahrlässigkeit in die einfache Fahrlässigkeit zu bringen. Für mich geht das Ganze noch ein bisschen weiter ...“

Adrian Lingen:
„Wir machen aus ISO Normen und BSI-Katalogen pragmatische Ansätze für den Mittelstand.“

Maximilian Wölk:
„Wir wollen nicht das NO im Wort InNOvation sein. Spannend für mich ist daher, Wege zu finden, neue Technologien sicher einzusetzen.“

Forschungsprojekt

Im März 2016 ist drei Jahre laufende Projekt Telemedizinische Informationen bei medizinischen Notfällen (T.I.M.E.) gestartet. Die Leitung des Forschungsvorhabens übernimmt die Stabsstelle Telemedizin des Universitätsklinikums Münster (UKM) in Zusammenarbeit mit dem Lehrstuhl der Klinik für Unfall-, Hand- und Wiederherstellungschirurgie, dem Lehrstuhl der Klinik für Anästhesiologie, operative Intensivmedizin und Schmerztherapie/ UKM-Trainingszentrum, dem Institut für Medizinische Informatik, dem Institut für Biometrie und Klinische Forschung und dem Zentrum für Klinische Studien Münster. Weitere Projektbeteiligte sind das Deutsche Zentrum für Luft- und Raumfahrt e.V. (DLR), die DATATREE AG (DATATREE), die CompuGroup Medical Deutschland AG (CMG), VISUS Technology Transfer GmbH (VISUS) und die Akademie der Unfallchirurgie GmbH (AUC). Das Vorhaben wird aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) gefördert.

Übergreifendes Ziel des Kooperationsprojekts ist es, die Qualität, Sicherheit und Effizienz der Notfallversorgung mithilfe innovativer und nutzerorientierter Informations- und Kommunikationslösungen flächendeckend zu erhöhen.

Im Projekt T.I.M.E. wird dabei zwischen zwei Teilprojekten unterschieden. Das Teilprojekt „Notfalldaten“ untersucht in einer Simulationsstudie den Einfluss des Notfalldatensatzes auf die präklinische Versorgung. Dies geschieht vor dem Hintergrund der ab 01.01.2018 geplanten Bereitstellung des Notfalldatensatzes auf der elektronischen Gesundheitskarte. Außerdem beschäftigen sich die Akteure des Projekts damit herauszufinden, wie die Verfügbarkeit von Notfalldatensätzen erhöht werden kann.

Im Teilprojekt „Tele-Schockraum“ soll ein umsetzungsfähiges Konzept zur telematischen Unterstützung der Schockraumversorgung in regionalen und lokalen Traumazentren durch überregionale Traumazentren entwickelt und evaluiert werden. Durch Video- und Audiokommunikation sowie Datenübertragung von beispielsweise Bildgebung oder Befunden zwischen den Kliniken soll eine optimierte Betreuung von Schwerverletzten geschaffen werden. Das überregionale Traumazentrum unterstützt dabei die Schockraumversorgung in den peripheren Krankenhäusern. Mithilfe dieses Kooperationskonzepts soll künftig eine noch effizientere Schwerverletztenversorgung in der Fläche realisiert werden.

IT-Sicherheit – *Läuft* bei uns!

Netzwerk nrw.uniTS bestreitet auch sportliche Herausforderungen gemeinsam.

Unter dem Motto „IT-Sicherheit – Läuft bei uns!“ traf sich am Donnerstag die Mannschaft der nrw.uniTS zum AOK Firmenlauf in Bochum. Für nrw.uniTS starteten 13 Läuferinnen und Läufer von unseren Partnern if(is) – Institut für Internet-Sicherheit, dem Horst Görtz Institut für IT-Sicherheit und der DATATREE AG.

Initiative für Informationssicherheit startet erfolgreich

Der Mensch – die größte Schwachstelle der Informationssicherheit. So nutzen Hacker angeborene Verhaltensweisen aus.

Herr Müller aus der Finanzabteilung erhält eine E-Mail des Vorstands. Er sitze gerade in einer wichtigen Sitzung und müsse dringend eine Überweisung tätigen. Den Überweisungsschein mit seiner Unterschrift hat der Vorstand bereits beigefügt. Herr Müller hat ein paar Rückfragen zu der Überweisung und mailt ein paarmal mit ihm hin und her. Nachdem alle offenen Punkte geklärt sind, überweist Herr Müller den Betrag. Was er nicht weiß: Er ist gerade Opfer einer Social-Engineering-Attacke geworden.

„Unsere IT-Systeme sind heute so komplex, dass es am einfachsten ist, den Menschen zu hacken. Kriminelle nutzen hier angeborene Verhaltensweisen aus, um ihr Ziel zu erlangen“, startet Sascha Czech, Bereichsleiter IT-Sicherheit der Sana Kliniken AG, seinen Vortrag über psychologische IT-Sicherheit. Er zeigt die Wege und Möglichkeiten Krimineller auf, die Psyche des Menschen zu knacken und so an sensible Informationen zu gelangen. Anschließend zeigt Jan Domnik, IT-Sicherheitsberater des Instituts für Sicherheit und Datenschutz im Gesundheitswesen, wie einfach es ist, Privatpersonen zu hacken – und das selbst dann, wenn diese vermeintlich wenige Informationen über sich preisgeben. Darüber hinaus gibt er einen Einblick in die Macht von neuronalen Netzen und appelliert damit an eine gewisse Grundskepsis gegenüber Computern und die Sensibilisierung eines jeden Einzelnen.

Mitarbeitern Ängste nehmen

Das zweite Treffen der Initiative für Informationssicherheit im Gesundheitswesen beschäftigte sich mit dem Schwerpunkt Social Engineering. Zur Steigerung des entsprechenden Bewusstseins muss zum einen Mitarbeitern die Angst vor dem Thema Informationssicherheit genommen werden! Denn auch wenn die wenigsten IT-Systeme heute noch im Detail verstehen, ist es nichtsdestotrotz möglich, sich zu schützen! Dieser Aufruf darf sich jedoch nicht nur an die Mitarbeiter richten, sondern muss zum anderen von der Geschäftsführung mit der nötigen Aufmerksamkeit betrachtet werden. Die Veröffentlichung der entwickelten Leitsätze folgt in Kürze.

Sie möchten mitwirken?

Die finale Ausarbeitung der Arbeitsergebnisse und Arbeitsgruppenberichte wird zeitnah veröffentlicht. Sie möchten zukünftig alle Ergebnisse aus erster Hand erhalten? Hierzu bieten wir Ihnen zwei Möglichkeiten.

1. Als Verantwortlicher für den Bereich IT-Sicherheit in Ihrer Einrichtung haben Sie die Möglichkeit, sich aktiv an der Arbeitsgruppe zu beteiligen. Beantragen Sie jetzt formlos die Aufnahme in den Arbeitskreis.
2. Melden Sie sich zu unserem kostenlosen Informationsangebot der Initiative für Informationssicherheit im Gesundheitswesen an.

Mitglieder der Initiative sind:

- Diakonisches Werk Bethanien e.V.
- Institut für Sicherheit und Datenschutz im Gesundheitswesen
- KIT Services GmbH – Knappschaft Bahn See
- Kliniken Essen-Mitte – Evang. Huyssens-Stiftung/ Knappschaft GmbH
- Krankenhaus-Kommunikations-Centrum
- Sana Kliniken AG
- Serapion

Das nächste Treffen der Initiative für Informationssicherheit im Gesundheitswesen wird am **26.09.2017** in Solingen stattfinden.

Anmeldungen nimmt Nina Richard unter **richard@isdsg.de** gerne entgegen.

Lesen Sie mehr ab Seite 17

Das Datenschutz-managementsystem

Mit der Europäischen Datenschutzgrundverordnung (EU-DSGVO) wird Datenschutz zum Managementthema. Um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu evaluieren, wird ein Datenschutzmanagementsystem (DSMS) notwendig. Wir geben Ihnen eine erste Hilfestellung.

Am 25. Mai 2016 ist die Europäische Datenschutzgrundverordnung (EU-DSGVO) in Kraft getreten. Sie gilt nach einer zweijährigen Übergangsfrist unmittelbar in der gesamten Europäischen Union. Ziel ist es, das Datenschutzrecht innerhalb Europas stärker zu vereinheitlichen. Die nationalen Umsetzungen der Datenschutzrichtlinie aus dem Jahr 1995 führten trotz aller Harmonisierungsbemühungen nur bedingt zu einem einheitlichen Datenschutzniveau in der Europäischen Union. Vielmehr gibt es einen Flickenteppich von datenschutzrechtlichen Regelungen. Mit der EU- DSGVO gelten zukünftig in allen Staaten der Europäischen Union grundsätzlich die gleichen Standards (Heft 6 bfdi).

Prinzipien der Datensparsamkeit, der Angemessenheit und Erforderlichkeit, der Transparenz und Zweckbindung, der Gewährleistung der Datensicherheit sowie der unabhängigen Aufsicht bleiben den deutschen Unternehmen als Vorgaben erhalten.

Neu hinzugekommen sind Grundsätze wie Privacy by Design und Privacy by Default, das Marktortprinzip sowie das Recht auf Vergessenwerden. Auch der Bereich der Sanktionierung von Datenschutzverstößen ändert sich. Wo bisher maximal 300.000 € Bußgeld fällig werden konnten, werden mit der DSGVO Bußgelder in Höhe von bis zu 4 % des weltweiten Konzernumsatzes möglich. Dies macht die Implementierung eines Datenschutzmanagementsystems notwendig.

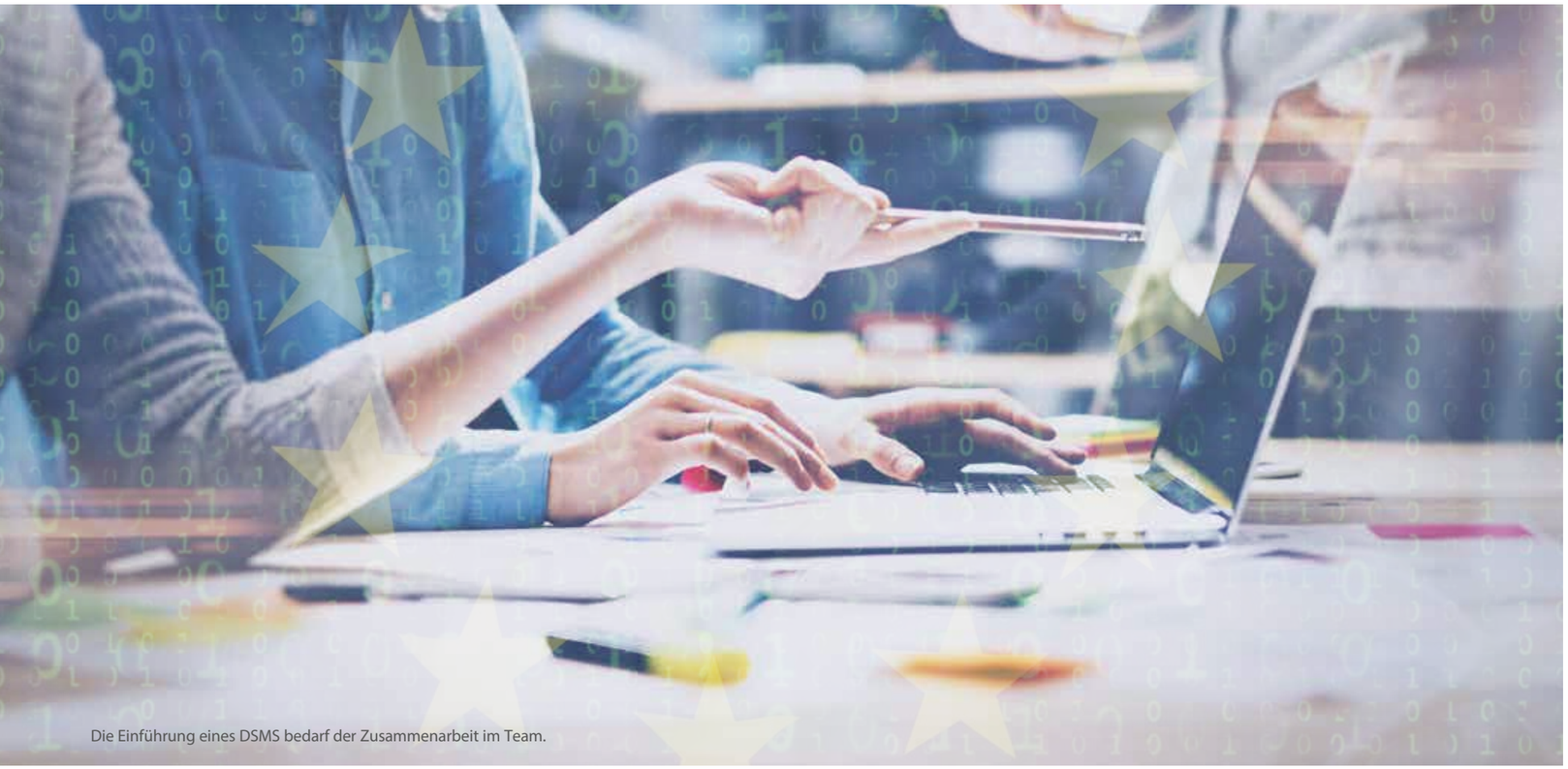
Was ein DSMS nicht ist

Im ersten Schritt gilt es, die Begrifflichkeit des Datenschutzmanagementsystems zu definieren. In der Praxis scheint in einigen Kreisen der Begriff fälschlicherweise als ein IT-System zum Management des Datenschutzes verstanden zu werden. Ein IT-System ist allerdings nicht mehr als ein unterstützendes Tool, um Prozesse, Maßnahmen und Aufgaben im Rahmen der Qualitätssicherung innerhalb des Datenschutzes abzubilden. Das DSMS beschreibt allerdings einen Managementansatz zur Implementierung des Datenschutzes in die Organisationsstruktur.

Verschaffen Sie sich einen Überblick

Zur Implementierung eines Datenschutzmanagementsystems gilt es, Ihre Organisation zu kennen. Der Einstieg mithilfe eines Unternehmensorganigramms ist eine fundierte Basis. Nicht selten stellt das Organigramm ausschließlich hierarchische Ebenen des Unternehmens dar. Prüfen und erstellen Sie deshalb darüber

> *Die Umsetzung der Anforderungen aus der Europäischen Datenschutzgrundverordnung stellt eine zeitintensive und anspruchsvolle Aufgabe dar.*



Die Einführung eines DSMS bedarf der Zusammenarbeit im Team.

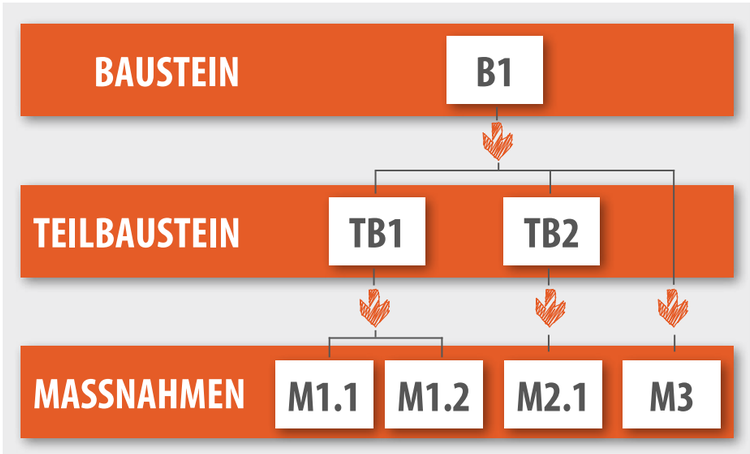
hinaus dar, welche Prozesse in Ihrer Einrichtung existieren und welcher Kollege hier agiert. Erarbeiten Sie dies gemeinsam mit den Fachabteilungen. Prüfen Sie auch, an welcher Stelle Daten verarbeitet werden. Diese ausgearbeitete Übersicht dient als Basis für Ihre weitere Arbeit.

Allgemeines zum Vorgehen

Als Basis sollten Sie zunächst definieren, welche Strukturen, Prozesse, Rollen und Verantwortliche relevant sind. Das zentrale Element des DSMS ist die Dokumentation. Ihre Dokumentation sollte gemäß Best-Practice-Beispielen aufgebaut sein. Ergänzend hierzu gilt es, einen Anforderungskatalog zu entwickeln, der sich gesetzlichen und Anforderungen der Informationssicherheit widmet. Den aktuellen Managementsystemen liegt zumeist das Model des PDCA-Zyklus zugrunde.

Prozesse und Maßnahmen

Die Umsetzung der Anforderungen aus der EU-Datenschutzgrundverordnung stellt eine zeitintensive und anspruchsvolle Aufgabe dar, die ein strukturiertes Vorgehen, ein stimmiges Vorgehensmodell und ein durchdachtes Projektmanagement erfordert.



Maßnahmen des DSMS ergeben sich aus der EU-DSGVO.

Zu Beginn steht die Identifikation der Prozesse und Maßnahmen, die für das Unternehmen relevant sind, denn nicht für jedes Unternehmen sind alle Prozesse und Maßnahmen umzusetzen. Setzt beispielsweise ein Unternehmen keine Dienstleister zur Verarbeitung von personenbezogenen Daten ein bzw. wird nicht als Dienstleister durch einen Verantwortlichen eingesetzt, ist das Thema Auftragsverarbeitung für das Unternehmen nicht von Relevanz.

Die Struktur zur Gliederung der einzelnen Anforderungen aus der Europäischen Datenschutzgrundverordnung sollte wiefolgt aufgebaut sein:

BAUSTEIN
Ein Baustein ist eine thematische Einordnung von Teilbausteinen oder Maßnahmen, welche sich aus den Anforderungen der Europäischen Datenschutzgrundverordnung sowie von Prozessen im Unternehmen ergeben.

TEILBAUSTEIN
Ein Teilbaustein dient zur feineren Einordnung von Maßnahmen.

MASSNAHME
Eine Maßnahme ist ein konkreter Umsetzungshinweis, der die Anforderung aus einem oder mehreren Artikeln der Europäischen Datenschutzgrundverordnung erfüllt. Die Beschreibung jeder einzelnen Maßnahme erfolgt anhand des nachfolgenden Schemas.

So beschreiben Sie Maßnahmen

Die Maßnahmenbeschreibung beginnt mit einer Erörterung der Anforderung(en) aus der Europäischen Datenschutzgrundverordnung.

Und welche Maßnahme setze ich als Erstes um?

Nutzen Sie einheitliche und gängige Begrifflichkeiten. Hierzu ist es hilfreich, die von Ihnen genutzten Fachtermini für Ihre Organisation zu definieren.

VERANTWORTLICHE
Erläutert die für die Umsetzung der Maßnahme und Einhaltung der Anforderung verantwortlichen Personen innerhalb des Unternehmens.

ANFORDERUNGEN
Beschreibt die Referenz von einem oder mehreren Artikeln der Europäischen Datenschutzgrundverordnung.

ÖFFNUNGSKLAUSEL
Zeigt an, ob für die referenzierte Anforderung aus der EU-DSGVO eine Öffnungsklausel besteht.

VERKNÜPFUNG
Stellt zwischen der vorliegenden Maßnahme und einer oder mehrerer weiterer Maßnahmen eine thematische Verbindung her.

Zur Identifikation der Maßnahmen, welche zur Umsetzung der Europäischen Datenschutzgrundverordnung durchgeführt werden müssen, dient eine Auflistung der Maßnahmen. Anhand der Auflistung und Analyse der Maßnahmen wird entschieden, ob die jeweilige Maßnahme für die Umsetzung im Unternehmen relevant ist oder nicht. So werden sukzessiv alle umzusetzenden Maßnahmen identifiziert.

Nachdem die Auswahl aller relevanten Prozesse und Maßnahmen durchgeführt wurde, stellt sich die entscheidende Frage: Und welche Maßnahme setze ich als Erstes um?

Diese Frage lässt sich nicht pauschal für jede Einrichtung beantworten, denn das Datenschutzniveau ist in jedem Unternehmen auf einem anderen Level. Aus diesem Grund ist eine Priorisierung der Maßnahmen sinnvoll. Das Ziel dieser Priorisierung ist eine Liste, welche alle Maßnahmen auflistet und diese absteigend nach ihrer Umsetzungsdringlichkeit sortiert.

Die Priorisierung der Maßnahmen

erfolgt auf Grundlage von zwei definierten Parametern:

AUFWAND
Der Parameter *Aufwand* unterteilt sich sowohl in den *monetären* als auch in den *zeitlichen* Aufwand. Auf Grundlage dessen sollte dann eine sinnvolle Aufwandsabschätzung durchgeführt werden.

SCHADENSAUSWIRKUNG
Bei der Beurteilung der Schadensauswirkung sollten Sie eine Unterteilung in *äußere und innere Konsequenz* vornehmen. *Innere Auswirkungen* sind beispielsweise Produktions- bzw. Dienstleistungsstillstand, Verlust von personenbezogenen Daten. Bei *äußeren Konsequenzen* handelt es sich beispielswiese um Kontrollen und Strafen durch Aufsichtsbehörden oder Imageverlust.

Für die Bewertung von *Aufwand und Schadensauswirkung* pro Maßnahme empfiehlt es sich, aus Gründen der Übersichtlichkeit eine Tabelle zu erstellen.

Nachdem der Aufwand und die Schadensauswirkung für jede Maßnahme bzw. jeden Prozess bewertet wurden, erfolgt die eigentliche Priorisierung.

Eine Liste mit den Maßnahmen sowie einer Priorisierung hinsichtlich der Umsetzung im Unternehmen hat mehrere Vorteile:

PROJEKTPLANUNG
In erster Linie ist die Liste zur eigentlichen Projektplanung zur Umsetzung der Europäischen Datenschutzgrundverordnung gedacht. Sie bietet eine Übersicht aller umgesetzten und noch umzusetzenden Maßnahmen inklusive einer Priorisierung der Umsetzung an.

AUFSICHTSBEHÖRDEN
Meldet sich eine Aufsichtsbehörde zur Visite während der Umsetzungsphase an, kann durch die Liste dargestellt werden, dass die umzusetzenden Maßnahmen identifiziert wurden. Außerdem ist nachzuvollziehen, auf welcher Grundlage die Entscheidung zur Umsetzung der einzelnen Maßnahmen geschehen ist.

MANAGEMENT-SUMMARY
Das Management hat die Möglichkeit, jederzeit Einblick in die Projektfortschritte zu nehmen.

Mit diesem Vorgehensmodell haben Sie bereits einen kleinen Schritt Richtung Datenschutzmanagemensystem gemacht. ■

Nina Richard

Dr. Christian Stoffers

leitet das Geschäftsführungsreferat Kommunikation & Marketing der St. Marien-Krankenhaus Siegen gem. GmbH, eines integrierten Gesundheitsunternehmens mit circa 2.000 Mitarbeitern. Er ist stellvertretender Vorstandsvorsitzender des Zentrums für die Digitalisierung der Wirtschaft Südwestfalen und Dozent im Studiengang Medizinische Informatik an der Universität Siegen. Zuvor zeichnete er als Pressesprecher für die Vorstandsabteilung Public Relations der Impress Software AG, Hannover/Boston, verantwortlich.

Im Inte rview mit Dr. Christian Stoffers

Marketing & Datenschutz – ist hier ein Miteinander möglich?

Marketing und Datenschutz – häufig eine Beziehung, die nicht unbedingt auf einer engen Zusammenarbeit beruht. Zwei völlig unterschiedliche Welten, die aufeinandertreffen und oft Schwierigkeiten haben, eine gemeinsame Sprache zu finden. Es kann aber auch funktionieren – bestes Beispiel: das St. Marien-Krankenhaus Siegen. Lesen Sie mehr in unserem Interview mit Dr. Christian Stoffers.

Widersprechen sich die Themen Datenschutz und Marketing für Sie?
Einen Widerspruch kann ich nicht ausmachen. Besondere Berührungspunkte sehe ich insbesondere bei den Marketinginstrumenten „Promotion“ und „Process“. Um zu verhindern, dass eine komplexe Kommunikationskampagne am Ende aufgrund von Verstößen gegen datenschutzrechtliche, wettbewerbsrechtliche oder urheberrechtliche Anforderungen scheitert oder sich das Krankenhaus mit teuren Abmahnungen konfrontiert sieht, sollte der Datenschutzbeauftragte selbstverständlich von Anfang an in die Planung einbezogen werden.

Zudem erfordert das Thema Medizin 4.0, das insbesondere die Customer Journey betrifft, einen engen Schulterschluss von Marketer und Datenschützer.

Was sind hier die größten Herausforderungen für die Marketingwelt in Krankenhäusern?
Die größten Herausforderungen sind im Naturell der Marketer zu finden. Nicht selten handelt es sich bei ihnen um kreative Köpfe, die schnell von der eigenen Idee oder dem Impuls ihrer Agentur begeistert sind. Planvolles Handeln wird zu gerne dem Effekt untergeordnet. Es muss also schon bei der Planung einer Marketingmaßnahme kritisch hinterfragt werden, was beispielsweise mit den hieraus gewonnenen Daten gemacht werden soll. Nur so kann die kreative Idee so umgesetzt werden, dass das Krankenhaus tatsächlich etwas mit den gewonnenen Daten machen darf.

Weiter „leben“ Marketer vom Überraschungsmoment, was sie gegenüber anderen im Krankenhaus agierenden Bereichen bis zum Rollout einer Maßnahme verschlossen macht. Damit es da kein böses Erwachen gibt, muss frühzeitig der Datenschutzbeauftragte einbezogen werden.

Teilen Sie diese Ansichten?
Uneingeschränkt ja. Der Datenschutzbeauftragte muss frühzeitig einbezogen werden; so macht man ihn zum ziemlich besten Freund der Marketingabteilung.

Wie gut läuft die Kommunikation zwischen Ihnen und Ihrem Datenschutzbeauftragten?
In vielen Unternehmen sind die Marketer und der Datenschutzbeauftragte nicht gerade beste Freunde. Das ist nicht nur sehr schade, sondern es schadet; eine gute Zusammenarbeit kann dem Krankenhaus auch eine Menge Ärger ersparen.

Ich lege daher Wert auf eine gute Kommunikation mit dem Datenschutzbeauftragten. Diese erfolgt institutionalisiert zum Beispiel über die Arbeitsgruppe IT-Sicherheit, aber auch im direkten Gespräch im Rahmen der Projektplanung.

Wie sähe die perfekte Zusammenarbeit zwischen Datenschutz und Marketing/Kommunikationsabteilung aus?
Meines Erachtens sind beide Seiten gefordert. Sowohl der Datenschützer als auch der Marketer verfolgen neue Entwicklungen zum Beispiel im Bereich der Internettechnologien. Die wechselseitige Information schon vor einem konkreten Bedrohungsszenario würde das dringend notwendige Vertrauen festigen.

Welchen Rat würden Sie Datenschutzbeauftragten mit auf den Weg geben, um die Kommunikation mit Marketingmenschen zu verbessern?
Der Datenschutzbeauftragte sollte sich auch von neuen Ideen begeistern lassen und die ehrliche Begeisterung auch dem Marketer vermitteln. Er handelt als „Freund und Helfer“ und unterstützt als solcher die Umsetzung der Maßnahme.

Ein Freund kann selbstverständlich auch eine klare Ansage machen, wenn eine Kampagne von vornherein zum Scheitern verurteilt ist. ■

Interview: Nina Richard

Nutzen Sie die Synergien mit Ihrer Marketingabteilung?

Die Integration des Datenschutzes in die Unternehmenskommunikation hat viele Vorteile. Wird sie nicht beachtet, kann das enorme negative Konsequenzen haben. In der Praxis gestaltet sich die Kooperation der Unternehmensbereiche Kommunikation und Datenschutz jedoch oft schwierig. Warum aber auch der Datenschutzbeauftragte von einem guten Draht zur Kommunikationsabteilung profitiert, wird im folgenden Text erläutert.

Werden Sie Teil der internen Unternehmenskommunikation

Für Ihre tägliche Arbeit ist es wichtig, dass Sie den Datenschutz, und seine Grundsätze kommunizieren, und zielgruppengerecht aufbereiten und der Zielgruppe zugänglich machen. Gar nicht so leicht, ein auf den ersten Blick trockenes Thema spannend zu vermitteln. Setzen Sie sich deshalb mit Ihren Kollegen aus der internen Unternehmenskommunikation zusammen und überlegen sich ein Konzept, um beispielsweise das Bewusstsein Ihrer Einrichtung für das Thema zu steigern oder das Thema Datenschutz allgemein präsenter zu machen.

Datenschutz in der externen Unternehmenskommunikation

Für die externe Unternehmenskommunikation ist es wichtig, die Öffentlichkeit mit aktuellen und relevanten Informationen rund um die eigene Institution zu versorgen, um so verschiedene Ziele, wie die Information der Bevölkerung, die Bekanntmachung neuer Behandlungsmethoden oder aber auch die lückenlose Information von Patienten und Angehörigen zu Ärzten zu erreichen.

Der Datenschutz muss hier ähnlich wie im Marketing begleitend erfolgen, um beispielsweise die Website der Institution, Regelungen für die elektronische Kommunikation oder Terminvereinbarungen datenschutzkonform zu gestalten.

Datenschutz im Marketing und Marketing im Datenschutz

Aus Sicht des Datenschutzbeauftragten ist die Unternehmenskommunikation/Marketingabteilung häufig die Abteilung, die gegen das Prinzip der Datensparsamkeit verstößt. Ziel ist es, die Zielgruppe bestmöglich zu kennen, um ihr genau das Informationsangebot zur Verfügung zu stellen, das sie braucht, und eine möglichst persönliche Beziehung aufrechtzuerhalten. Hierzu sind personenbezogene Daten vorteilhaft. Versuchen Sie als Datenschutzbeauftragter deshalb, die Sicht der Marketer zu verstehen und nicht, deren Arbeit zu verhindern, sondern bemühen Sie sich um gemeinsame Lösungen für ein effizientes Arbeiten. Darüber hinaus: Lassen Sie sich ein paar Tricks und Kniffe von Ihren Marketerkollegen zeigen – auch Sie haben Zielgruppen, die Sie erreichen müssen. ■

Nina Richard

So bauen Sie einen Draht zu Ihren Kollegen auf

Der Datenschutzbeauftragte ist eine Institution innerhalb eines Unternehmens, die allzu oft nur als „Kontrollorgan“ und damit als „Feind“ gesehen wird. Er kontrolliert die Kollegen und gibt Anweisungen, wie etwas durchzuführen ist. Aber hinter einem DSB steckt noch mehr – er/sie ist eine Vertrauensperson, ein Mentor, ein Analyst. Der Vielfältigkeit innerhalb eines Unternehmens hinsichtlich der Charaktere sämtlicher Mitarbeiter muss er ebenso differenziert entgegentreten. Aber wie baut ein DSB einen Draht zu den Kollegen auf?

Jeder Mensch tickt anders

Die Herausforderung für den Datenschutzbeauftragten lautet: Jeder Mensch tickt anders. Die Denkweise der Kollegen ist zum Beispiel abhängig vom ausgeübten Beruf, vom Bildungsstand ebenso wie vom Alter oder dem Geschlecht. Dass bedeutet für den DSB, dass er sich auf jeden Menschentyp einstellen können sollte und im Vorfeld von zum Beispiel Mitarbeiterschulungen zum Datenschutz entsprechende Informationen über die Teilnehmer einholen muss.

Sind die Teilnehmer aus der IT-Abteilung, dann benötigen diese vielleicht eher Schulungsthemen aus dem Rechtsbereich. Mitarbeiter aus anderen Bereichen wissen zwar, dass sie personenbezogene Daten verarbeiten, haben aber nicht die technischen Kenntnisse, um diese ausreichend zu schützen. Dann muss der Datenschutzbeauftragte Themen zu den eingesetzten IT-Systemen und entsprechende Schutzmaßnahmen schulen.

Mitarbeiter erreichen, aber wie?

1. Schulungen

Das Mittel der Wahl, um viele Menschen persönlich zu erreichen, sind Mitarbeiterschulungen. In diesen können anschauliche Datenschutzbeispiele vorgebracht und in relativ kleiner und damit persönlicher Runde diskutiert werden. Eine praxisnahe Schulung bleibt in den Köpfen der Mitarbeiter hängen und kann sogar das „öde“ Thema Datenschutz so lebendig machen, dass sich die Mitarbeiter gerne für eine nächste Schulung zu diesem Thema anmelden.

> *Bei Datenschutzschulungen muss auf das Klientel geachtet werden. Für die Managerebene sind andere Inhalte als für die Mitarbeiterebene erforderlich.*

Geachtet werden muss bei Datenschutzschulungen auf die Klientel: Auf der Managementebene erfordert ein Datenschutzvortrag sicherlich andere Inhalte als auf der Ebene der Mitarbeiter, die keine Berührungspunkte mit dem Management (zum Beispiel Ärzte, Krankenschwestern, Callcentermitarbeiter) haben.

2. Persönliche und vertrauliche Gespräche

Der DSB, ob betrieblich oder extern bestellt, sollte immer für ein vertrauliches Gespräch für alle Mitarbeiter zur Verfügung stehen. Dabei versteht es sich von selbst, dass der DSB der Schweigepflicht unterstellt ist und die Kollegen daher vertrauensvoll an ihn herantreten können. Der DSB muss sich neutral und unabhängig verhalten und diese Stellung gegenüber der Geschäftsleitung und den Mitarbeitern leben.

3. Infobriefe per Mail, per Aushang

Einen Draht zu den Kollegen sämtlicher Abteilungen aufbauen, bedeutet natürlich auch, sie über Neuerungen oder besonders brisante Datenschutzthemen kontinuierlich zu informieren. Dabei ist es hilfreich, diverse Medien wie Newsletter, Artikel in Firmenzeitschriften oder Aushänge einzusetzen.

Fazit:

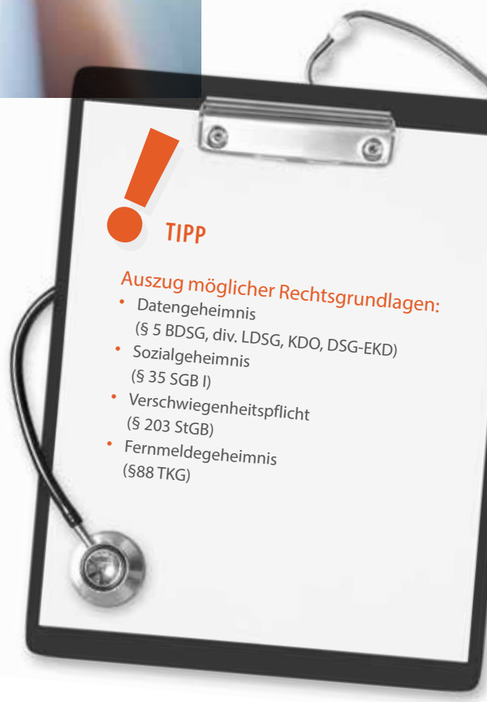
Der Draht zu den Mitarbeitern wird durch Vertrauen und Präsenz aufgebaut. Dies gelingt durch regelmäßige Schulungen, mittels wiederholter Präsenz in den Unternehmensmedien und durch Vertrauen. Arbeiten Sie darauf hin, als Vertrauensperson wahrgenommen zu werden und auch ausreichend Beachtung beim Management zu erhalten. Nur so kann das Thema Datenschutz in Ihre Organisation integriert werden. ■

Susann Zorbach

Behalten Sie den Überblick über gesetzliche Anforderungen.

7. Goldene Regel: Verpflichten Sie Ihre Mitarbeiter

Die Verpflichtung von Mitarbeitern auf das Datengeheimnis spielt von jeher eine wichtige Rolle im Datenschutz. Neben den Datenschutzgesetzen, die diese Verpflichtung auf Bundes- oder Landesebene sowie bei den Kirchen kennen, gibt es auch die Verpflichtung auf branchenspezifische Gesetze, wie zum Beispiel auf das Sozialgeheimnis oder die Verschwiegenheitspflicht. Doch ist neben der gesetzlichen Grundlage auch die richtige Form und Art der Verpflichtung entscheidend.



Rechtsgrundlage

Bevor die Mitarbeiter verpflichtet werden können, muss zuerst die Rechtsgrundlage geklärt werden. Außerdem spielt die jeweilige Tätigkeit des Mitarbeiters eine Rolle bei der Verpflichtung, so sind Mitarbeiter, welche in die Verarbeitung von Sozialdaten involviert sind, zusätzlich auf das Sozialgeheimnis zu verpflichten. Um bei der Verpflichtung von Mitarbeitern nicht lange nach den jeweiligen Rechtsgrundlagen suchen zu müssen, ist das Zusammenfassen von Tätigkeiten in Rollen für die Verpflichtung zu empfehlen.

Gestaltung der Verpflichtung

Die Mitarbeiter sind schriftlich zu verpflichten. Zudem ist die Verpflichtung in einer laienverständlichen Sprache zu verfassen. Referenzierte Gesetzestexte sind im Sinne der Transparenz als Anhang an die Mitarbeiter auszuhändigen. Die unterschriebene Verpflichtungserklärung ist als Dokumentation in der Personalakte des Mitarbeiters abzuheften.

> **Welche Mitarbeiter sind zu verpflichten?**
>
> Hinsichtlich der Gesetzgebung findet keine Unterscheidung bezüglich des Anstellungsverhältnisses der Mitarbeiter statt, welche an der Datenverarbeitung beteiligt sind. Demnach sind alle Mitarbeiter unabhängig des Anstellungsverhältnisses (Auszubildende, Aushilfen, studentische Hilfskräfte, Leiharbeiter, Vorstand etc.) zu verpflichten.

EU-DSGVO und Mitarbeiterverpflichtung

Aus der Europäischen Datenschutzgrundverordnung kann implizit die Verpflichtung der Mitarbeiter aus Artikel 24 abgeleitet werden. Dort sieht die Gesetzgebung vor, dass der Verantwortliche u. a. organisatorische Maßnahmen zum Schutz der Daten trifft. Eine Verpflichtung der Mitarbeiter stellt eine solche Maßnahme dar. Die novellierte Fassung des BDSG, das BDSG-neu, sieht wiederum eine explizite Verpflichtung der Mitarbeiter gemäß § 53 vor.

Wir empfehlen daher, die Verpflichtungserklärung bestehen zu lassen. Hierbei sind nur entsprechend die gesetzlichen Grundlagen anzupassen. ■

Alexander Vogel

Informationssicherheit

Die Komplexität von digitalen Technologien schreit nach strukturierter Informationssicherheit.

Mehr Initiative für Ihre Informationssicherheit

Gemeinsam haben wir uns zum Ziel gesetzt, strukturierte Informationssicherheitsmaßnahmen und Handlungsempfehlungen zu erarbeiten. Das Know-how der Experten von großen Klinikverbänden und kleineren Einrichtungen macht die Initiative besonders effizient und hilfreich.

Die jüngsten Vorfälle haben gezeigt, dass niemand von uns sicher vor Hackerangriffen ist. Die Auslegung innerhalb der Medien war dabei nicht immer ganz korrekt. Dies führt zu Zweifeln an Deutschlands Krankenhäusern und der Sicherheit der hoch sensiblen Gesundheitsdaten. Diesem Bild soll mit der Initiative für IT-Sicherheit im Gesundheitswesen öffentlichkeitswirksam entgegengewirkt werden.

Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen möchte deshalb einen Zusammenschluss von IT-Verantwortlichen, Geschäftsführern und Datenschutzbeauftragten herbeiführen, um Transparenz und Aufklärungsarbeit im Bereich der IT-Sicherheit zu schaffen. Es sollen so praxisnahe Handlungsempfehlungen für die Krankenhauslandschaft entwickelt werden.

Ziele der Initiative:

- Verbesserung der Reputation von Krankenhäusern in Bezug auf die IT-Sicherheit
- Erarbeitung von Grundsätzen zur Lage der IT-Sicherheit in Krankenhäusern
- Krisenfälle bestmöglich vermeiden
- Stärkung des Bewusstseins für IT-Sicherheit
- Öffentlichkeitswirksame Pressearbeit
- Optional Entwicklung einer Kampagne zur IT-Sicherheit

Sie möchten mitwirken?

Die finale Ausarbeitung der Arbeitsergebnisse und Arbeitsgruppenberichte wird zeitnah veröffentlicht. Sie möchten zukünftig alle Ergebnisse aus erster Hand erhalten? Hierzu bieten wir Ihnen zwei Möglichkeiten.

Als Verantwortlicher für den Bereich IT-Sicherheit in Ihrer Einrichtung haben Sie die Möglichkeit, aktiv an der Arbeitsgruppe teilzunehmen. Beantragen Sie jetzt formlos die Aufnahme in den Arbeitskreis.

Melden Sie sich zu unserem kostenlosen Informationsangebot der Initiative für Informationssicherheit im Gesundheitswesen an.

Mitglieder der Initiative sind:

- Diakonisches Werk Bethanien e.V.
- Institut für Sicherheit und Datenschutz im Gesundheitswesen
- KIT Services GmbH – Knappschaft Bahn See
- Kliniken Essen-Mitte – Evang. Huyssens-Stiftung/Knappschaft GmbH
- Krankenhaus-Kommunikations-Centrum
- Sana Kliniken
- Serapion

Nina Richard

Gemeinsam sind wir stark!

Wie sicher sind Informationen, oder was ist es uns wert, uns anvertraute Informationen sicher aufzubewahren?

Stimmen aus den eigenen Reihen

Jeden Tag kann man in der Presse lesen, dass es wieder Cyberattacken auf Unternehmen aus Industrie und Gesundheitswesen gegeben hat. Diese mögen gezielt oder ungezielt sein, aber sie hinterlassen in der Regel immer einen Schaden und zwar nicht nur in Netzwerken oder auf Servern. Sie hinterlassen auch, im übertragenen Sinne, Spuren im Gedächtnis der betroffenen Menschen. Jeden Tag werden uns sensible Daten von Menschen anvertraut, diese dürfen mit Recht erwarten, dass wir mit diesen Daten sorgfältig umgehen und alles dafür tun, dass diese nicht in unbefugte Hände fallen. Der Gesetzgeber gibt uns mit dem IT-Sicherheitsgesetz einige Hausaufgaben auf: Jedes Krankenhaus muss sich dieses Themas annehmen. Natürlich spielen Budget und Ressourcen zur Umsetzung eine große Rolle, aber auch mit kleinem Budget und wenig Ressourcen lässt sich schon einiges bewegen. Die Dringlichkeit sollte jedem Verantwortlichen klar sein. Die Frage ist nur, wie kann man es umsetzen und wen kann man fragen?

Die Initiative für Informationssicherheit im Gesundheitswesen kann hierbei unterstützen; sie vereint Vertreter größerer und kleinerer Häuser sowie Verbände und Beratungshäuser. Man kann sich über bereits implementierte Lösungen, aber auch über vorhandene, spezifische Eigenheiten des eigenen Unternehmens austauschen. Da dieser Austausch auf Gegenseitigkeit beruht, kann jeder vom Anderen lernen.

Hier werden einerseits Vorträge zu verschiedenen Themen zur IT-Sicherheit gehalten, andererseits Vorschläge und Checklisten erarbeitet, die Unternehmen der Gesundheitsbranche eine große Hilfestellung sein können.

Frank Krause

Frank Krause
IT-Leiter

Alle Einrichtungen des Diakonischen Werkes Bethanien haben den gemeinsamen diakonischen Auftrag „leben helfen“. Das heißt hinschauen und begleiten, hinhören und beraten, pflegen und heilen, trösten und fördern. Die Arbeit ist seit Bestehen des über 100-jährigen Werkes von der Überzeugung geprägt, dass jeder Mensch unendlich wertvoll ist.

Erpressungstrojaner von der Stange

Meinungsmacher prägen unsere Ansichten und Bilder von Sachverhalten, dabei vergessen wir manchmal, nach rechts und links zu schauen und die uns vorliegenden Informationen objektiv zu bewerten und für uns zu beurteilen. Lassen Sie uns doch gemeinsam einmal die Augen schließen und uns einen Hacker vorstellen …

Der klassische Cyberkriminelle trägt Kapuzenpulli und Anonymous-Maske, sitzt in einem dunklen Verschlag oder Keller und konsumiert Pizza und Cola. Selbstverständlich ist er sozial inkompatibel und fällt durch seine Unscheinbarkeit schon fast wieder auf. Am wohlsten fühlt er sich vor seinem Monitor und tummelt sich in millionenzeiligem Quellcode im Darknet.

Cyberkriminelle Machenschaften sind schon längst gesellschaftsfähig.

Wenn das Ihrem Bild des Hackers unserer Zeit entspricht, muss ich Sie leider enttäuschen – was vielen nämlich noch nicht bewusst ist: Cyberkriminelle Machenschaften sind schon längst gesellschaftsfähig.

Kannten Sie AlphaBay?

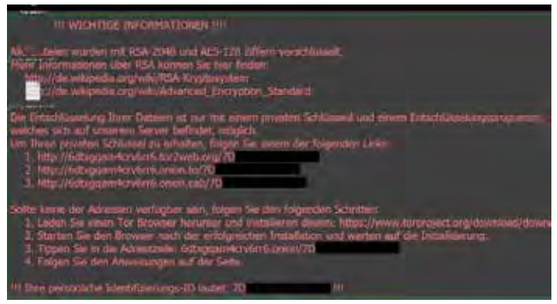
Von seinem Aufbau und der Funktionsweise war AlphaBay vergleichbar mit eBay – mit kleinen bedeutenden Unterschieden. AlphaBay war der, nach Produktlistings, größte Darknet-Markt. Gehandelt wurde alles von Waffen über Auftragsmorde, Kreditkarteninformationen bis hin zu Drogen und verschreibungspflichtigen Medikamenten. Gezahlt wurde anonym mit der digitalen Währung Bitcoins oder Monero. Die Qualitätsbewertung der Abwicklung und des Händlers erfolgte per Sternchen im Händlerprofil.

Der Betrieb des Marktplatzes AlphaBay wurde im Juli 2017 von der Justiz eingestellt.

Das Ende des Darknets?

Der Betrieb des Marktplatzes AlphaBay wurde im Juli 2017 von der Justiz eingestellt. Wer jetzt denkt, dass das Darknet hiermit am Ende ist, liegt falsch – die Maschinerie bietet

Die Ähnlichkeit mit gängigen Online-Händlern ist unverkennbar. Das gibt ein Gefühl für die Professionalität, die dahintersteckt.



PC gehackt? Jetzt gilt es, schnell zu handeln.

Quelle: Wikipedia

eine Vielzahl von Alternativplattformen, die weiterhin für die genannten Zwecke genutzt werden können.

Innerhalb der Marktbetrachtung kann man vier verschiedene Arten von Marktbeziehungen unterscheiden:

1. **C2C – Customer-to-Customer**
   Hackerangriff zwischen Privatpersonen
2. **C2B – Customer-to-Business**
   Privat organisierte Hacker (Skript-Kiddys oder auch der typische Innentäter) versuchen, Unternehmen anzugreifen
3. **B2C – Business-to-Costumer**
   Professionelle Hackerorganisationen oder Geheimdienste versuchen, Privatperson anzugreifen
4. **B2B – Business-to-Business**

Dezidierte Marktbetrachtung

Unser kleiner thematischer Ausflug in die Welt des Darknets hat uns gezeigt, wie komplex und professionell organisiert das Darknet mit seinen kriminellen Marktteilnehmern ist.

Simplizität von Angriffen

Ein beliebtes Angriffsszenario zur Infektion eines IT-Systems ist die klassische E-Mail mit infiziertem Link oder Anhang. Im besten Fall wird die Systeminfektion von dem Mitarbeiter selbst oder den IT-Sicherheitsverantwortlichen bemerkt, bevor die Verschlüsselung der Systeme ihren Lauf nimmt. Das Entdecken solcher Angriffe wird aufgrund der zunehmenden Systemkomplexität und der Professionalität der Angreifer immer herausfordernder. Heutzutage müssen Hacker nicht mehr professionell in der Programmierung von Schadsoftware sein. Der Hang zu kriminellen Machenschaften oder eine gewisse Grundwut auf den Arbeitgeber können schon völlig ausreichen. Anschließend kann sich direkt an der Vielzahl der existierenden Ransomwarebaukästen bedient werden.

Seien Sie auf Angriffe vorbereitet

Im Falle eines erfolgreichen Angriffs zum Beispiel mit einem Verschlüsselungstrojaner wird dieser langsam aber sicher Ihre Daten verschlüsseln. Die meisten Hacker sind keine Unmenschen und bieten Ihnen selbstverständlich die Möglichkeit, Ihre Daten wieder freizukaufen.

Ist es soweit gekommen, gilt es nur noch zu reagieren. Hierzu bestehen drei Möglichkeiten:

1. Unproblematisch ist es, wenn Sie über ein sehr gut funktionierendes Backup-Konzept verfügen und Ihre Backups noch nicht von dem Verschlüsselungstrojaner befallen sind.
2. Auch kann versucht werden, Ihre Daten wieder zu entschlüsseln. Hierzu gibt es einige Unternehmen am Markt, die sich darauf spezialisiert haben.
3. Sie zahlen das geforderte Lösegeld per Bitcoins. Allerdings ist es in der Regel nicht empfehlenswert, Erpressern ohne Weiteres ein Lösegeld zu zahlen.

Empfehlenswert ist es, sich auf jeden Fall professionelle Unterstützung zu holen und sowohl das Bundeskriminalamt als auch das BSI zu informieren. Hier bekommen Sie neutrale und kompetente Unterstützung.

Besser als Nachsorge bleibt die Vorsorge

Besser als das bloße Reagieren auf Angriffe ist natürlich die proaktive Vorbereitung der gesamten Einrichtung, sprich Prozesse, Mitarbeiter, Management vorab so zu sensibilisieren, dass Angriffe erkannt werden, bevor Sie erfolgreich sein können.
Machen sie sich bewusst, dass IT-Sicherheit ein Managementthema ist. Um Ihre Einrichtung strukturiert in Hinblick auf die IT-Sicherheit zu verbessern, kommen Sie deshalb um ein Informationssicherheitsmanagement nicht herum. Hierzu

Machen Sie sich bewusst, dass IT-Sicherheit ein Managementthema ist.

stehen Ihnen zwei etablierte Standards zur Verfügung:

1. ISO 27001
2. BSI Grundschutz

Beide Ansätze sind sehr umfangreich, wobei der BSI Grundschutz so viele personelle und zeitliche Ressourcen in Anspruch nimmt, dass er für kaum eine Einrichtung praktikabel und aus diesem Grund praxisfern ist. Nicht umsonst gibt es für diesen Ansatz mehr Auditoren als auditierte Unternehmen. Die Auditierung nach ISO 27001 ist um einiges praktikabler, jedoch noch immer sehr umfangreich, sodass Sie bei einem ISMS nach ISO 27001 auch ein relativ großes Budget benötigen. Allerdings ist insbesondere bei kleinen Einrichtungen ein großes Budget für die Informationssicherheit nicht gegeben.

Ausschließlich für Unternehmen, die aktuell unter KRITIS fallen, ist eine Zertifizierung nach ISO verpflichtend. Für alle anderen Unternehmen sind die Anforderungen nicht immer umsetzbar. Nutzen Sie deshalb Kompromisslösungen, die in Anlehnung an einen der vorgestellten Ansätze erarbeitet werden. ■

Jan Domnik

IT-Sicherheit: „Investieren Sie richtig?“

Die Anforderungen an den Schutz und die Absicherung von IT-Infrastrukturen haben in den letzten Jahren signifikant zugenommen und damit auch die Nachfrage nach Experten, die Einrichtungen hierbei unterstützen: Der Markt reagiert, und Anbieter von Hard- und Software für eine sichere IT-Infrastruktur schießen aus dem Boden und offerieren eine breite Palette, die den IT-Sicherheitsverantwortlichen zu einem einfachen Job verhelfen sollen. Doch tragen diese Tools tatsächlich zur Lösung von IT-Sicherheitsproblemen bei oder können Sie Ihr Budget doch sinnvoller einsetzen?

Der Irrglaube, die eigene IT-Infrastruktur sei durch eine Firewall und einen Antivirenscanner gänzlich abzusichern, hält sich auf der Managementebene hartnäckig. Zur Freude von übereifrigen Vertrieblern, die sich in diesem Bereich spezialisiert haben. Allerdings sind die Zeiten, in denen diese Komponenten ausreichend waren, um vor komplexen Angriffsmethoden zu schützen, längst vorbei. Mit der zunehmenden Vernetzung und Digitalisierung von Unternehmen sowie Prozessen sind auch Cyberkriminelle längst dahintergekommen, ihre Techniken zu erweitern und die Vernetzung und Digitalisierung als Schwachstelle der Kernprozesse anzusehen und hieraus ihr Kapital zu schaffen.

Lassen Sie sich nicht auf falsche Versprechungen ein

Der Bedarf an der Etablierung von ganzheitlichen Abwehr- und Schutzmaßnahmen steigt. Die Schnelllebigkeit und Komplexität der Branche führen dazu, dass Entwicklungen häufig selbst am Management vorbeirasen. Anrufe der Vertriebsteams von IT-Sicherheitsunternehmen, die versuchen davon zu überzeugen, dass nur kostspielige Investitionen vor Cyberangriffen schützen können, gelten in Expertenkreisen eher als kontraproduktiv. Denn diese Art von Investitionen ist oftmals, ohne ein ganzheitliches und strukturiertes Vorgehen, ein Tropfen auf den heißen Stein und nichts weiter als eine Ergänzung der IT-Sicherheit. Um die komplexe Maschine IT-Sicherheit zu warten und zu schützen, bedarf es allerdings fundierter Fach- und Detailexpertise des Informationssicherheitsbeauftragten/CISO, der jedes Zahnrad seiner Maschine kennt, sie ölt und dafür sorgt, dass alle Teile aufeinander abgestimmt sind und reibungslos ineinandergreifen. Dabei stehen Verantwortlichkeiten innerhalb des Unternehmens, Konzepte und Prozesse im Vordergrund. Nur wer in einem Notfall auch weiß, was er zu tun hat, kann entsprechend richtig reagieren und erforderliche Maßnahmen einleiten. Hierzu kann nur ein Managementsystem für Informationssicherheit eine sinnvolle Basis sein. Zum Start in die strukturierte Informationssicherheit helfen drei Punkte:

- Unabhängige Berater
- Strukturen und Prozesse kennen
- Penetrationstests und Maßnahmen aus dem Social Engineering

Unabhängige Berater

Um einen neutralen Blick mit viel Erfahrung auf Ihre Einrichtung zu erhalten und darüber hinaus (falls gewünscht oder verpflichtend) auf eine Zertifizierung hinzuarbeiten, bietet es sich an, einen externen Berater oder Auditor hinzuzuziehen. Dieser sollte dabei nicht nur Erfahrungen im Audit-Bereich vorweisen können, sondern gleichzeitig auch über fundiertes Know-how im Bereich der IT verfügen. Legen Sie großen Wert auf dessen Unabhängigkeit – nur so können Sie sicher sein, dass Sie neutral beraten werden, ohne dass der Vertrieb von Sicherheitstools beabsichtigt wird. Darüber hinaus kennt er in der Regel verschiedene Ansätze von Informationssicherheitsmanagementsystemen und wählt für Sie das richtige Vorgehensmodell aus.

Der Vorteil eines externen Beraters – er ist innerhalb Ihrer Organisation nicht so bekannt wie Sie es sind. Gerade wenn es später darum geht, Angriffe zu simulieren, kann dies vorteilhaft sein, um unverfälschte Ergebnisse zu erzielen.

Das BSI hat hierzu eine Empfehlung für zu treffende Vereinbarungen zwischen Ihnen und dem Dienstleister veröffentlicht:

- Verschwiegenheitspflichten
- Einsatz von Hard- und Software und die zu testenden IT-Systemen und IT-Anwendungen
- Festlegung von erlaubten und unerlaubten Aktivitäten der Penetrationstester, um Schäden möglichst zu vermeiden
- Vereinbarungen über den Umgang mit Datenträgern vor, während und nach Abschluss des Penetrationstests, da die Datenträger zum Beispiel sensible Informationen über die Testergebnisse enthalten können
- Festlegungen über den Ort der Durchführung sowie zur Auswertung und Berichterstellung für den Penetrationstest
- Festlegung eines Terminplans einschließlich Wartungsfenster für die Durchführung der Tests
- Detaillierte Vereinbarungen über den Zugang zum Internet bzw. den Anschluss von Testsystemen an das Internet während der Durchführung und der Auswertung von Penetrationstests
- Vereinbarungen über Zuständigkeiten und die Erreichbarkeit von Ansprechpartnern sowie zur Notfallvorsorge[1]

Strukturen und Prozesse kennen

Sie selbst sollten für Ihre eigene Arbeit die Strukturen und Prozesse Ihrer Einrichtung sowohl auf technischer als auch auf organisatorischer Ebene berücksichtigen. Hilfreich sind hier Informationen über Abteilungen, Ansprechpartner und sowie über die eingesetzte Soft- und Hardware etc.

Penetrationstests

In der klassischen Betrachtung gelten Penetrationstests als ein Vorgehen, um den Stand der Sicherheit von IT-Systemen festzustellen und die möglichen Risiken aufzuzeigen. Zieht man den Definitionsrahmen etwas weiter, können auch Verfahren des Social Engineerings hierunter gefasst werden.

Schritt 1: Informationssammlung
Die Ist-Aufnahme ist die erste Handlung, die der externe Berater durchführen soll. Anhand von öffentlichen Quellen und internen Mitarbeitern versucht der externe Berater, so viele Informationen über die Einrichtung/das Angriffsziel zu erhalten wie nur möglich ist. Es folgt die Berichterstattung, in der die potenziellen Schwachstellen ausgewertet werden.

Schritt 2: Angriffssimulation
Durch die gesammelten Informationen kann mit den Eindringungsversuchen in die Infrastruktur oder das Unternehmen begonnen werden.

Schritt 3: Handlungsempfehlungen
Nach erfolgter Durchführung des Penetrationstests werden die Ergebnisse analysiert und bewertet. Hieraus leiten sich konkrete Maßnehmen und Umsetzungszeitpläne – je nach Risiko der erkannten Schwachstellen – ab.

Was habe ich davon?

Die hieraus erlangten Ergebnisse dienen der strukturierten Verbesserung Ihrer Informationssicherheit. Zum einen haben Sie eine Übersicht inklusive konkreter Handlungsempfehlungen, um potenzielle Sicherheitslücken zu schließen. Nutzen Sie darüber hinaus die Ergebnisse, um die notwendige Managementunterstützung für Ihren Bereich bei der Geschäftsführung einzuholen. Zum anderen wissen Sie, wie Sie Mitarbeiter geeignet sensibilisieren.

Erst, wenn Ihr Unternehmen ein verlässliches ISMS aufgebaut hat, kommt die Kür – und damit die Überlegung, ob es sinnvoll ist, IT-Sicherheitstools einzusetzen, die helfen Prozesse zu automatisieren und im Detail auf die Anforderungen des Unternehmens abgestimmt sind. Wirklich sinnvoll sind die Investitionen in die IT-Sicherheit, die auf Ihr Unternehmen und dessen Anforderungen abgestimmt sind. ■

Sascha Czech

Weiterführende Informationen:

1 Quelle https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05150.html)

Sascha Czech ist Information Security Officer bei der Sana Kliniken AG. Die Sana Kliniken AG ist als drittgrößte private Klinikgruppe Deutschlands einer der bedeutendsten Anbieter im Bereich integrierter Gesundheitsleistungen. Die Sana Kliniken AG wurde 1976 gegründet und ist nicht börsennotiert. Ziel ist Spitzenmedizin in einem breiten Versorgungsangebot.

Der Informationssicherheitsbeauftragte

Aufgaben und Kerntätigkeiten des Informationssicherheitsbeauftragten

Der Chief Information Security Officer, kurz CISO, kann als Pendant zum Datenschutzbeauftragten im Bereich der Informationssicherheit gesehen werden. Die formelle deutsche Bezeichnung, die zum Beispiel im Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme zu finden ist, lautet Informationssicherheitsbeauftragter.

Ein Informationssicherheitsbeauftragter sollte benannt werden. Vorlagen für eine Bennenungsurkunde stellt das BSI zur Verfügung. Als Informationssicherheitsbeauftragter agieren Sie als Stabsstelle zur Geschäftsführung, deren Kernaufgabe darin besteht, Informationen bzw. Assets angemessen zu schützen.

> *Ein Informationssicherheitsbeauftragter agiert als Stabsstelle zur Geschäftsführung.*

Der Aufgabenbereich des Informationssicherheitsbeauftragten (ISB) umfasst alle Beratungs- und Unterstützungsleistungen, die sich unmittelbar aus den maßgeblichen gesetzlichen Verpflichtungen im Rahmen des Risikomanagements ergeben, insbesondere im Hinblick auf die nachfolgenden Erfordernisse:

- Schutz von Informationen bzw. Assets der Institution
- Überprüfung und Evaluierung sicherheitsrelevanter Betriebsprozesse
- Vertraulichkeit, Integrität sämtlicher Daten
- Verfügbarkeit der IT-Infrastruktur
- Reduzierung der im Schadensfall entstehenden Kosten
- Sicherstellung der Kontinuität der Arbeitsabläufe
- Erhaltung der in Technik, Informationen, Arbeitsprozessen und Wissen investierten Werte
- Wirtschaftlichkeit der Schutzmaßnahmen
- Kompetenz der Mitarbeiter im Bereich Informationssicherheit

Die konkreten Tätigkeiten des Informationssicherheitsbeauftragten können, je nach Größe und Aufbau einer Organisation, stark voneinander abweichen. Während er in größeren Institutionen eine koordinierende Rolle einnimmt, ist er in kleineren Institutionen dagegen auch für die Ausführung des IT-Tagesgeschäfts tätig.

> *Die Tätigkeiten des Informationssicherheitsbeauftragten können je nach Organisation stark voneinander abweichen.*

Bei der Wahrnehmung seiner Aufgaben beeinflusst der Informationssicherheitsbeauftragte die IT-Strategie des Unternehmens.

Eine enge Abstimmung mit den dafür verantwortlichen Stellen, wie dem Chief Information Officer (CIO), stellt somit ebenfalls einen Teil der Arbeit des Informationssicherheitsbeauftragten dar.

Die Kerntätigkeiten des ISB sind daher in der Regel die folgenden:

- Implementierung und Betrieb eines Managementsystems für Informationssicherheit, zum Beispiel in Anlehnung an die Norm ISO 27001
- Implementierung der Sicherheitsstrategie durch eine Sicherheitsleitlinie und dazugehörige Konzepte, Regelungen und Richtlinien, Arbeitsanweisungen und Schulungen
- Audits auf technischer Ebene zur Gewährleistung der IT-Sicherheit
- Audits auf der organisatorischen Ebene in den Bereichen Governance, Risk und Compliance
- Information der Leitungsebene, des IT-Verantwortlichen und des Datenschutzbeauftragten über den Status quo der Informationssicherheit
- Koordination sicherheitsrelevanter Projekte
- Untersuchung von Sicherheitsvorfällen
- Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit
- Unterstützung bei der Erarbeitung und Definition der sicherheitsrelevanten Objekte, der Bedrohungen und Risiken und der daraus abgeleiteten Sicherheitsziele
- Unterstützung beim Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele und Ausarbeitung relevanter Sicherheitsvorschriften
- Prüfung der Funktionseinheiten zum Stand der Umsetzung und Weiterentwicklung der Sicherheitsvorschriften.

Impressum

ExperSite Ausgabe 02 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, kb-photodesign/Monkey Business Images ; S. 3: Falko Wübbecke, Dortmund; shutterstock Pressmaste/kb-photodesign; S. 4/5: F. Wübbecke, Dortmund, B. Sandrock; S. 6: nrw.uniTS ; S. 7: shutterstock, Mix and Match Studio; S. 8: shuttestock, SFIO CRACHO/kb-photodesign, S. 10: shutterstock, SFIO CRACHO/kb-photodesign; S. 11: C. Stoffers; S. 14: shutterstock, Monkey Business Images; S. 15: shutterstock, sdecoret, LZ Image; S. 16: shutterstock, Mikko Lemola; S. 17: F. Krause; S. 18: shutterstock, Rawpixel.com; S. 20: shutterstock, Rawpixel.com; S. 21: S. Czech Sana Kliniken AG; S. 22/23: shutterstock, ink drop; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke

"It's our new security software. That's what happens if the system detects unauthorized access to patient records."

Für die inhaltliche Mitgestaltung möchten wir uns herzlich bei nachfolgenden Gastautoren bedanken:

Sascha Czech, Sana Kliniken AG
Frank Krause, Diakonie Bethanien
Dr. Christian Stoffers, St. Marien-Krankenhaus Siegen

Die nächste Ausgabe erscheint im März 2018

Schwerpunkt:
Endspurt für die Datenschutzgrundverordnung. Diese Sofortmaßnahmen sollten Sie jetzt noch umsetzen.