ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 02 2018

APOKALYPSE DATENSCHUTZ

Besinnen wir uns doch einfach mal wieder auf das Wesentliche

Konzepterstellung leicht gemacht
Mit diesen Leitfäden gelingen Ihnen Datenschutz- und IT-Sicherheitskonzepte

Hackerspielerei: Pentesting
Sicherheitslücken finden und schließen

Branchenübergreifend lernen
So funktioniert Informationssicherheit bei einem Chemielogistik-Dienstleister

Inhalt

Versuchen Sie, sich der Panikmache rund um die DSGVO zu entziehen.

Wie werde ich als Datenschutzbeauftragter zum Kommunikator?

Informationssicherheit – die richtige Auswahl für Ihre Maßnahmen treffen.

Impressum

ExperSite Ausgabe 02 2018 | 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: S. 2: shutterstock, pathdoc; Pixabay, bogitw; shutterstock, Sergey Nivens; S. 3: Falko Wübbecke, S. 4: shutterstock, panuwat phimph; S. 5: Datatree AG; unsplash, andrik langfield; S. 6: Falko Wübbecke, S. 7: unsplash, isaac benhesed, jeshoots.com; S. 11: shutterstock, Mentari Merah Studio; S. 12: shutterstock, Panchenko Vladimir ; S. 13: ZTG GmbH; S. 14: Grafik prolytics market research GmbH, S.15: Grafik prolytics market research GmbH, shutterstock, Rawpixel.com; S. 16–19: shutterstock, Sergey Nivens; S. 20: A. TALKE GmbH & Co KG; Pixabay, Pascal Treichler; S. 22: Pixabay, bogitw.

JETZT KOMMEN SIE MIR NICHT MIT:

„Wir können ja bald gar nicht mehr arbeiten“

Liebe Leserinnen, liebe Leser,

sie kam angerollt und hat uns alle überrascht. Naja, eigentlich nicht, denn die Europäische Datenschutz-Grundverordnung war kein spontanes Unterfangen, die Übergangsfrist zwei Jahre im Vorfeld angezählt. Und dennoch führte sie mit dem 25. Mai 2018 zu großer Überraschung für viele Unternehmen.

Was war passiert und wem ist es zu verdanken?
Apokalyptische Propheten dominierten die Medien und vermittelten das Gefühl, der Weltuntergang stünde kurz bevor, gleichzeitig boten sie gegen den Einwurf von Münzen und Scheinen die eine Lösung an, die die Menschheit retten könne.

Nahezu jedes Unternehmen im B2B-Bereich versuchte, auf den Zug aufzuspringen. Nicht nur jeder Unternehmensberater konnte plötzlich im Datenschutz beraten, auch eine Vielzahl von Softwareanbietern versprach: „Mit uns sind Sie perfekt auf die DSGVO vorbereitet.“

Das ist jetzt Ihre Chance für einen Neuanfang.
Auf der Strecke blieb dabei recht häufig der eigentliche Grundgedanke des Datenschutzes. Einhergehend mit der falschen Erwartung, Datenschutz sei eine Sache, die „mal eben“ erledigt werden könne, ergaben sich tolle Geschäftsmodelle für schwarze Schafe. Aber konzentrieren wir uns doch mal wieder auf das Wesentliche und stellen die Frage:

Warum machen wir das eigentlich alles?

Auf gesetzlicher Ebene sind es aller Wahrscheinlichkeit nach wirtschaftliche Faktoren, die Sie dazu bringen, sich mit dem Thema Datenschutz auseinanderzusetzen. Auf persönlicher Ebene sind wir aber selbstbestimmte Menschen, die nicht sorglos mit ihren Daten umgehen sollten, um Firmen nicht zu Weltmächten und uns selbst zu Marionetten zu machen. Und plötzlich sind wir wieder auf der beruflichen Ebene, wo jeder von uns mit hochsensiblen Gesundheitsdaten arbeitet und dort ebenfalls eine große Verantwortung für diese Daten hat.

Jetzt kommen Sie mir nicht mit: „Wir können ja bald gar nicht mehr arbeiten“.

Klar können wir und wir werden. Gemeinsam schaffen wir das.

N Richard

Ihre Nina Richard
Redaktionsleitung

ePrivacy – konkretere Lösungen für mehr Verbraucherschutz

Die Europäische Datenschutz-Grundverordnung gilt an vielen Stellen als zu allgemein, sodass es zu spezifischen Regelungen für Einzelfälle kommen muss. Insbesondere der Umgang mit elektronischen Kommunikationsmedien kommt zu kurz. Experten auf allen Ebenen fordern hier konkrete Regelungen.

Der Gesetzgeber arbeitet bereits seit Januar 2017 an einer neuen Verordnung, die die ePrivacy-Richtlinie 2002/58/EG ablösen soll. Ursprünglich hätte die Verordnung zusammen mit der EU-DSGVO in Kraft treten sollen. Hier kam es allerdings zu Verzögerungen, die u. a. dem Regierungsbildungsprozess geschuldet sind.

Schon wieder eine Verordnung?
Die ePrivacy-Verordnung spezifiziert die EU-DSGVO in Hinblick auf die Vorgaben privacy by design und privacy by default, d. h. in Bezug auf die datenschutzfreundliche Gestaltung und Entwicklung von Software. Die Verordnung wird ebenso wie die EU-DSGVO anzuwenden sein:

- Sie gilt unmittelbar für alle Mitgliedsstaaten,
- Sie muss nicht in national geltendes Recht umgesetzt werden,
- Strafen betragen je Verstoß bis zu vier Prozent des weltweiten Vorjahresumsatzes bzw. bis zu 20 Millionen Euro,
- Sie soll die unterschiedlichen Vorgaben und das Vorgehen der EU-Mitgliedsstaaten vereinheitlichen.

Durch das in Deutschland gültige TMG (Telemediengesetz) ist es beispielsweise möglich, Cookies per Opt-out-Regelung ohne die aktive Zustimmung des Nutzers einzusetzen. In anderen Mitgliedsstaaten bedarf es dagegen der aktiven Zustimmung (Opt-in-Regelung).

Darüber hinaus sollen viele derzeit vorhandene Grauzonen, wie die Datensicherheit bei Kommunikationsdiensten oder der Umgang mit personenbezogenen Daten im Onlinebereich, beseitigt werden. Auch in Bezug auf ein großes Problem vieler Softwarehersteller, wie das „Recht auf Vergessenwerden" sollen endlich konkretere Handlungsunterstützungen gegeben werden. Hieraus leiten sich neue Datenbank- und Kommunikationsstrukturen für Unternehmen ab. Datenbanken müssen beispielsweise so angelegt sein, dass alle sechs Monate ein Widerruf und damit das Löschen (auch aus allen Backup-Systemen) möglich ist.

Dies kann zur Folge haben, dass einige Gesetze, wie

- § 7 III UWG
- §§ 91 ff TKG
- §§ 11 ff TMG

ihre Gültigkeit verlieren.

Das Inkrafttreten der ePrivacy-Verordnung ist voraussichtlich für Ende 2019 geplant. Darüber hinaus ist wieder mit einer Übergangsfrist von zwei Jahren zu rechnen.

Umzug der Dortmunder Niederlassung

Die DATATREE AG mit dem Dienstleistungsbereich des ISDSG (Institut für Sicherheit und Datenschutz im Gesundheitswesen) bezieht im Dezember 2018 mit ihrer Dortmunder Niederlassung neue Räumlichkeiten und setzt damit ihren Wachstumskurs fort.

Die Mietflächen werden gemäß der Anforderungen der unterschiedlichen Geschäftsbereiche renoviert und befinden sich in der **Märkischen Str. 212–218**.

Sportlich unterwegs

GEMEINSAM SIND WIR STARK.

Der Teamgedanke steht bei der DATATREE AG ganz oben. Nicht nur die unterschiedlichen fachlichen Schwerpunkte im Datenschutz und der Informationssicherheit machen das Team und die Fachexpertise einzigartig.

Der Teamgedanke hört allerdings nicht mit dem Feierabend auf und so werden regelmäßig in der Freizeit die Sportschuhe geschnürt. Egal, ob es ein gemeinsames Volleyball-Match ist oder man sich in der Laufgruppe zur Vorbereitung auf den nächsten Firmenlauf trifft. „Wir sind ein eingespieltes Team, das sich nicht nur im Berufsalltag aufeinander verlassen kann", sagt Katrin Feyder, Officemanagerin und lizenzierte Fitnesstrainerin.

Ebenso vielfältig wie jeder Mitarbeiter, sind auch die Sportarten, die betrieben werden: von Volleyball, Mountainbiken, Klettern, Aerobic oder Triathlon bis hin zu Schach oder dem ambitionierten Marathonlauf. Der schönste Ausklang für ein gemeinsames, sportliches Event ist zudem ein gemeinsamer Abend bei Kaltgetränken und einer Wurst vom Grill.

EIN TAG MIT ...

CHRISTINE THIEME – BERATERIN DATENSCHUTZ

Ich treffe mich mit Christine Thieme am Düsseldorfer Standort der DATATREE AG. Wir arbeiten seit 2015 zusammen. Seit 2013 ist sie bei der DATATREE AG tätig. Als ich um 7.30 Uhr das Büro betrete, duftet es schon nach frisch gekochtem Kaffee und ich werde freudestrahlend begrüßt. Trotz eines vollen Terminplans bekomme ich einen Kaffee angeboten und wir unterhalten uns kurz über den bevorstehenden Urlaub und den Schulwechsel der Kinder. Ich war von dieser Frau schon immer begeistert, die gleichermaßen engagierte Mutter wie überragende Datenschutzberaterin ist.

Name
Christine Thieme

Studium
Diplom-Betriebswirtin, Bachelor of Arts (International Business), zertifizierte Datenschutzbeauftragte

Sprachen:
Deutsch, Englisch, Französisch

Beratungsschwerpunkt
Kunden- und Beschäftigtendatenschutz

Richard: ***Vielen Dank, dass Sie die Zeit für unser gemeinsames Interview gefunden haben. Gerade jetzt, nach Ende der EU-DSGVO-Übergangsfrist, ist diese doch bestimmt knapp bemessen?***
Thieme: Das wäre zu pauschalisiert betrachtet. Der Datenschutz hat sich schließlich nicht grundlegend verändert. Bereits vor Mai 2018 gab es Betroffenenrechte und Pflichten in Bezug auf die Auftragsverarbeitung, Grundsätze des Datenschutzes und noch vieles mehr. Was sich elementar verändert hat, sind die Höhen der möglichen Strafen für Datenschutzverstöße. Geldstrafen in Höhe von bis zu 20 Millionen Euro sind schon eine Hausnummer, weshalb das Thema Datenschutz plötzlich in das Bewusstsein von Unternehmen gerückt ist und in der Compliance-Struktur aufgeführt wird. Auch bei Dienstleistern wie Herstellern von Medizinsoftware spielt das Thema plötzlich eine große Rolle.

Wenn sich eigentlich nichts Grundlegendes im Datenschutz geändert hat, wie konnte das Thema DSGVO zu so einem Hype-Thema in der Presse werden?
Es war eine unglaubliche Entwicklung, dass ein Thema, das sonst so „unsexy" ist, es sogar bis in die Tagesschau geschafft hat. Jetzt könnte man meinen, dass uns Beratern für Datenschutzthemen doch nichts Besseres hätte passieren können. Da bin ich allerdings anderer Meinung. Denn für Berater, die die Philosophie haben, Datenschutz nicht als Verhinderer, sondern als prozessbegleitendes Thema zu sehen, das in die Unternehmenskultur integriert werden muss, war die Art und Weise der Berichterstattung häufig nicht wünschenswert. Reine Panikmache bringt den Datenschutz und seine Grundideen nämlich nicht weiter. Ich würde hier gerne ein Beispiel aufführen, um die Problematik zu verdeutlichen: Ein Kindergarten verschenkt an jedes Kind, das seine Kindergartenzeit beendet, ein liebevoll gestaltetes Abschiedsheft mit Bastelarbeiten und Fotos der Kinder und schwärzt unter dem Aspekt des Datenschutzes alle Gesichter. Ein perfektes Beispiel, das mit Datenschutz begründet wird, aber in der Realität nichts damit zu tun hat. „Das Recht am eigenen Bild" gab es nämlich bereits vor der Datenschutzgrundverordnung und ist im Kunsturhebergesetz geregelt. Solche Fälle, ebenso wie die Arzthelferin, die mir letztens eine vierseitige Datenschutzerklärung in die Hand drückte, da sie mir sonst nicht mein Rezept aushändigen könne, machen mir bewusst, wie viel Arbeit wir noch haben. Der Datenschutz wird durch falsche Berichterstattung und schwarze Beraterschafe in der Branche in falsches Licht gerückt. Denn diese genannten Beispiele haben nichts, aber wirklich gar nichts mehr mit den Grundsätzen des Datenschutzes zu tun.

Warum ein Job im Datenschutz?
Datenschutz ist ein unglaublich spannendes Themenfeld. Die Schnittstellen mit juristischen Ebenen und technologischen Entwicklungen in der Forschung oder der Telemedizin führen dazu, dass man regelmäßig neue Herausforderungen zu bewältigen hat. Und hier einen Ausgleich zwischen Arbeitserleichterung durch Technik und dem sensiblen Umgang mit beispielsweise Patientendaten zu finden, reizt mich. Hier muss es deutliche Regeln geben, die viel Arbeit erfordern, denn kein Fall ist wie der andere.

Der Job als Datenschutzberater, ist das schon immer Ihr Traumjob gewesen? Oder wie kommt man in die Branche?
(Lacht) Ich bin in einer Zeit groß geworden, in der es noch kein Internet gab. Sowohl während des Studiums als auch in meinen frühen Berufsjahren war Datenschutz nie ein Thema für mich. Als damals in meiner Firma das Internet eingeführt wurde, war ich als Teamleiterin tätig und habe erstmals eine E-Mail erhalten. Dieses Privileg wurde nur mir als Teamleiterin zuteil, da man noch die Kosten scheute, die dieser neumodische Kommunikationsweg mit sich brachte. Aber damals hätte ich nie gedacht, dass es möglich sei, personenbezogene Daten so zu verarbeiten, wie es heute gang und gäbe ist.

Ein freier Tag – wie verbringen Sie diesen?
An meinen freien Tagen hat meine Familie oberste Priorität. Wir sind sportlich viel unterwegs und genießen die Natur: Radtouren, Wandern, Schwimmen.

Jetzt mal Hand aufs Herz, Datenschutz ist jetzt nicht das Lieblingsthema beim Sonntagsfrühstück mit Freunden und Familie. Wie empfindet Ihr Umfeld das Thema?
Ach, das ist ganz unterschiedlich. Je besser sich die Menschen auskennen und je höher die Affinität zur IT ist, desto spannender ist das Thema auch. Je weniger Wissen in diesem Bereich vorherrscht, desto schwieriger ist es, Datenschutz als wichtiges Thema zu deklarieren. Ich versuche hier immer gerne, mit praktischen Beispielen aus Social Media und Technik zu vermitteln, dass mit wenig Aufwand bereits viel bewegt werden kann und die Einschränkung von Zugriffsrechten nicht gleich die Funktionalität von Gerätschaften beeinflusst.

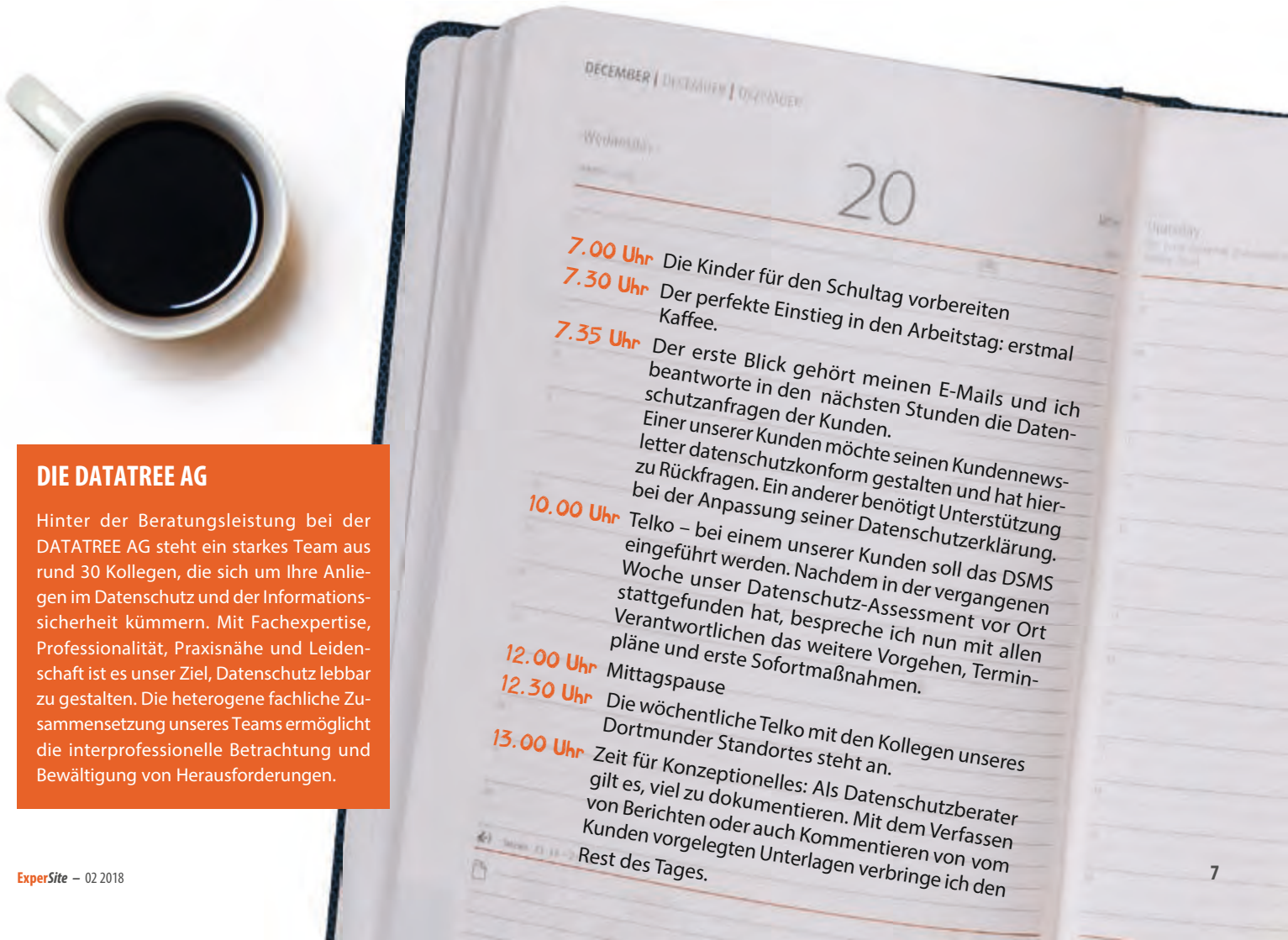
Ich komme hier in der Regel nicht drohend mit der Keule um die Ecke. Das stärkt nicht das Bewusstsein der Menschen, sondern nervt schlichtweg. Aber jeder Mensch muss die Eigenverantwortung für die Nutzung seiner Daten übernehmen.

Wer hat die Verantwortung für den Umgang mit Daten: Unternehmen oder Privatpersonen?
Unternehmen sind gesetzlich in der Pflicht. Aber nichtsdestotrotz bin ich als Privatperson aus meiner Sicht in der Pflicht, mich mit den Nachteilen oder „Gefahren" der Technik, die ich benutze, auseinanderzusetzen. Wenn ich mit dem Auto fahre, um die Vorteile der bequemen Fortbewegung zu nutzen, mache ich im besten Fall schließlich auch einen Führerschein und fahre nicht ungebremst mit 100km/h durch die nächste Kurve.

Haben Sie mit Vorurteilen zu kämpfen, wenn Sie das erste Mal einen Kunden besuchen?
Sowohl als auch. Die einen empfangen uns mit offenen Armen, weil sie wissen, dass sie Optimierungsbedarf haben und sind froh, dass sie jetzt von uns Unterstützung bekommen. Dann gibt es die Personen, die uns erstmal neutral gegenüberstehen, und natürlich die, die unsicher sind in Bezug auf die bevorstehenden Änderungen. Ich sehe es hier als unsere Aufgabe an, von vornherein unsere Werte zu vermitteln. Wir nehmen den Umgang mit personenbezogenen Daten ernst, aber auch die Herausforderungen, mit denen jeder Mitarbeiter zu kämpfen hat. Unsere Arbeit verbietet nicht – wir gestalten Prozesse, aber gemeinsam, und datenschutzkonform.

Warum sind Sie Datenschützerin?
Meine intrinsische Motivation ist schnell beschrieben. Es ist der spannendste Job, den ich je hatte! Ich möchte Datenschutz lebensnah gestalten. Genau das ist die Philosophie, die wir bei der DATATREE AG jeden Tag leben. ■

Interview: Nina Richard



DIE DATATREE AG

Hinter der Beratungsleistung bei der DATATREE AG steht ein starkes Team aus rund 30 Kollegen, die sich um Ihre Anliegen im Datenschutz und der Informationssicherheit kümmern. Mit Fachexpertise, Professionalität, Praxisnähe und Leidenschaft ist es unser Ziel, Datenschutz lebbar zu gestalten. Die heterogene fachliche Zusammensetzung unseres Teams ermöglicht die interprofessionelle Betrachtung und Bewältigung von Herausforderungen.

Akademie

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

SEMINARE

Europäische Datenschutz-Grundverordnung

Die Datenschutzgrundverordnung ist für die meisten Gesundheitseinrichtungen ein Großprojekt. Um die nötige Aufmerksamkeit dafür herzustellen, sind Praxisseminare unabdingbar. Wir bieten Ihnen:

- Gesetzliche Mitarbeiterunterweisung
- Grundlagenschulung für Mitarbeiter und Führungskräfte
- DSGVO für IT-Fachkräfte
- Informationssicherheit für Datenschutzbeauftragte

… u. v. m.

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.

STANDORTE: DÜSSELDORF, DORTMUND

U-STUNDEN: ca. 40 STUNDEN
U-ZEITEN: 4 FREITAGE

- **Der nächste Start ist für Februar 2019 geplant**

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

Datenschutzbeauftragter (BCW)

Das Thema Datenschutz ist so präsent wie nie. Mit Inkrafttreten der Europäischen Datenschutzgrundverordnung verzeichnen Unternehmen einen erhöhten Bedarf an Fachexperten, die die neuen Regularien praxisnah umsetzen.

Vom Internetauftritt des Unternehmens, über den richtigen Umgang mit Kundendaten, bis hin zur Einstellung neuer Mitarbeiter: Die neuen gesetzlichen Vorgaben verlangen ein ganzheitliches Datenschutz-Management-System, das Datenschutz zu einem Teil der Unternehmenskultur werden lässt.

Im Rahmen des zehnwöchigen berufsbegleitenden Lehrgangs Datenschutzbeauftragte/-r erlangen die Teilnehmer das notwendige Expertenwissen, um als gesetzlich geforderter Datenschutzbeauftragter unternehmensintern wie -extern agieren zu können. Neben juristischen und informationstechnologischen Kenntnissen steht dabei u. a. die Erweiterung kommunikativer sowie betriebswirtschaftlicher Kompetenzen auf dem Lehrplan.

BEGINN:
09.10.2018 IN ESSEN

Individuelle Workshops für Ihre Einrichtung

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

- Auftragsverarbeitung
- DSGVO
- Mitarbeiterschulungen
- Datenschutz
- Informationssicherheit

APOKALYPSE DATENSCHUTZ

Gegen Ende der Übergangsfrist der DSGVO kam schnell das Gefühl einer bevorstehenden Apokalypse und des Endes der Welt, oder sagen wir besser, der Geschäftstätigkeit vieler Unternehmen auf. Hier wird schnell übersehen, dass wir die DSGVO als echten Neuanfang nutzen können, um uns wieder auf die eigentlichen Grundsätze des Datenschutzes zu berufen, ohne falschen Propheten (oder Vertrieblern) Nährboden zu geben, die unter einer falschen Datenschutzflagge fahren.

Bereits zu Beginn des Jahres 2018 begannen einzelne Interessengruppen, sich mit dem Thema Datenschutzgrundverordnung auseinanderzusetzen. Schon zu diesem Zeitpunkt war es für die Unternehmen je nach Größe schwierig bis unmöglich, den geforderten ganzheitlichen Ansatz eines Datenschutz-Management-Systems umzusetzen. Erste Beiträge, die die DSGVO simpel erläuterten und fachlich objektiv über die bevorstehende Verordnung informierten, Änderungen aufführten und Begriffe erläuterten, wurden verbreitet. Im März 2018 erlebte die DSGVO dann einen Hype. Kurz vor Ende der Übergangsfrist im Mai veröffentlichte Studien, die darstellten, wie schlecht der Status quo der Umsetzung in deutschen Unternehmen tatsächlich war (vgl. Bitkom), ließen praktisch eine Welle der „Panik" losbrechen.

Jeder wollte ein Stück vom Kuchen haben

Jedes Unternehmen, von der Software- bis zur Beratungsbranche, versuchte, die Datenschutzgrundverordnung plötzlich als DAS Verkaufsargument zu nutzen. Guten Marketern wird hier schnell klar – ein USP (Unique Selling Proposition) gibt es nur so lange, wie die eigene Dienstleistung einzigartig ist. Dies führte uns zu einer erhöhten Nachfrage. Gemäß der mikroökonomischen polygopolen Marktgesetze folgte ein Anstieg des Angebots an Datenschutzberatern auf dem Markt.

Kurz gesagt: Plötzlich bot jeder an, die bevorstehende Verordnung unmittelbar umzusetzen. Das hat uns, mit Stand heute, vor allem eines gebracht, nämlich die Verzerrung der eigentlichen Datenschutzgrundsätze, wie beispielsweise Einfachheit und Transparenz, hin zu einem praxisfernen Bürokratieungetüm. Aus diesem Grund wird es Zeit, sich wieder auf das Wesentliche zu konzentrieren!

Worum geht es nochmal im Datenschutz?

Im Datenschutz geht es um das im Grundgesetz verankerte Recht, dass jede Person selbstbestimmt über die Verwendung ihrer personenbezogenen Daten entscheiden darf.

Personenbezogene Daten werden definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere durch die Zuordnung einer Kennung (…), identifiziert werden kann." Im Gesundheitswesen wird eine Vielzahl von Daten verarbeitet. Nicht zuletzt kommt noch eine Vielzahl von besonders schützenswerten Daten hinzu:

Als personenbezogene Daten der besonderen Art gelten Angaben zu

- der rassischen und ethnischen Herkunft
- der politischen Meinung
- der religiösen und weltanschaulichen Überzeugungen
- der Gewerkschaftszugehörigkeit
- genetische und biometrische Daten
- Gesundheitsdaten
- Daten über das Sexualleben/die sexuelle Orientierung

Alle personenbezogenen Daten unterliegen dem Verarbeitungsverbot mit Erlaubnisvorbehalt , d.h. dürfen nur aufgrund der Art. 6 Abs.1 a–f verarbeitet werden. Für personenbezogene Daten d. b. gibt es härtere Regeln.

Bei der täglichen Arbeit im Gesundheitswesen und mit den hier unterstützenden Technologien werden viele besonders schützenswerte Daten, beispielsweise Gesundheitsdaten, verarbeitet. So heißt es in der DSGVO:

> *Nach der DSGVO gehören Gesundheitsdaten zu den besonders schützenswerten Daten, für die ein grundsätzliches Verarbeitungsverbot besteht.*

„Im Sinne dieser Verordnung bezeichnet der Ausdruck: Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen."

Nach DSGVO gehören Gesundheitsdaten zu den besonders schützenswerten Daten, für die ein grundsätzliches Verarbeitungsverbot besteht. Eine Verarbeitung ist gemäß Art. 9 Abs. 2 DSGVO nur unter bestimmten Voraussetzungen möglich:

1. Es liegt eine Einwilligung des Betroffenen vor.
2. Es existiert eine andere gesetzliche Grundlage, die die Verarbeitung rechtfertigt.

Darüber hinaus ergeben sich folgende Grundsätze der Datenverarbeitung:

- **Transparenz** – es ist für den Laien verständlich, was mit seinen Daten geschieht.
- **Zweckbindung** – die Daten werden nur für den Zweck genutzt, für den sie auch erhoben wurden.
- **Datenminimierung** – es werden nur die Daten erhoben und verarbeitet, die wirklich zur Erfüllung des Geschäftszwecks nötig sind.
- **Richtigkeit** – Daten sind aktuell zu halten – alte, nicht mehr korrekte Daten sind zu löschen.
- **Speicherbegrenzung** – Daten dürfen nur solange gespeichert werden, wie es zur Erfüllung des Geschäftszweckes notwendig ist.
- **Integrität und Vertraulichkeit** – Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit und der Schutz vor unbefugten Dritten gewährleistet ist.

Personen, die sich bereits vor der DSGVO mit dem Thema Datenschutz auseinandergesetzt haben, wird auffallen, dass die Themen nicht neu sind.

Umso mehr verwundert es, dass die Neuerungen der DSGVO zu einer Art Panikmache genutzt wurden, denn die Grundidee Datenschutz war nie eine andere. Ein Argument, das wohl viele Geschäftsführer dazu brachte, sich mit dem Thema auseinanderzusetzen, ist der erweiterte Bußgeldkatalog, der Unternehmen dazu veranlasste, den Datenschutz in die Wirtschaftlichkeitsbetrachtung einzubeziehen – ein erster Erfolg für die Datenschützer.

Den größten und herausforderndsten Anpassungsbedarf haben wohl Anbieter und Hersteller von Software. In Hinblick auf die ePrivacy-Verordnung ist 2019 noch einiges zu erwarten.

Was Datenschutz allerdings nicht ist

Schauen wir uns nach drei Monaten Datenschutzgrundverordnung das Medienbild erneut an, erhalten wir Presse-Headlines wie „Kita schwärzt Kinderfotos aus Datenschutzgründen", „DSGVO: der Startschuss ging nach hinten los" oder „Abmahnwelle DSGVO". Das sind nur einige der Negativbeispiele, wie die DSGVO in der Praxis gelebt wird, die aber im Grunde nichts mehr mit Datenschutz zu tun haben. Nicht nur in den Medien trifft man plötzlich auf suspekte Datenschutzregelungen. Wenn beispielsweise die Mitarbeiter/-innen in Apotheken dazu angehalten sind, jedem Kunden eine mehr-

ENTWICKLUNG DES DATENSCHUTZES

Im Jahr 1970 wurde in Hessen das erste Datenschutzgesetz weltweit veröffentlicht. Es folgten weitere Gesetze von Bund und Ländern, die ein Korrektiv der im Zusammenhang mit den Terroraktionen der Roten Armee Fraktion eingeführten Rasterfahndung bildeten. Im Zusammenhang mit dem Datenschutz steht auch das Volkszählungsurteil von 1983 aus dem das Recht auf informationelle Selbstbestimmung abgeleitet wurde (Art. 2 GG).

Die Bedeutung des Datenschutzes spiegelte sich in den Bestrebungen wider, das Thema auf europäischer Ebene zu verankern. Aufgrund der unterschiedlichen politischen Interessen gestalteten sich die Verhandlungen kompliziert und langwierig.

Die Europäische Datenschutz-Grundverordnung trat am 24. Juni 2016 in Kraft und ist seit dem 25.Mai 2018 anzuwenden. Sie gilt unmittelbar für alle Mitgliedsstaaten, erfordert jedoch viele Anpassungen der Gesetze auf Bundes- und Landesebene.

Personen, die sich bereits vor der DSGVO mit dem Thema Datenschutz auseinandergesetzt haben, wird auffallen, dass die Themen nicht neu sind.

seitige Einwilligungserklärung in Schriftgröße zehn vorzulegen, geht dies gänzlich an allem vorbei, wofür Datenschützer sich Tag für Tag einsetzen: praxisnahe Lösungen für selbstbestimmtes Handeln im Umgang mit personenbezogenen Daten.

Wussten Sie, dass die Unkenntlichmachung von Fotos nichts mit der DSGVO zu tun hat?

Am Beispiel der bereits oben aufgeführten Kita wird besonders gut deutlich, dass alte Themen unter der Flagge der DSGVO neu verkauft und falsch interpretiert werden. Der Grund: Unwissenheit und Berater, die versuchen, Profit aus einer Notsituation zu generieren. Das Recht am eigenen Bild beispielsweise ist nicht in der DSGVO begründet, sondern resultiert aus dem Kunsturhebergesetz. Ähnlich verhält es sich mit Hinweisen auf Cookies, Webseitenverschlüsselung oder die Datenschutzerklärung und dem Telemediengesetz.

So sollte es nicht sein

Aus Angst, die neuen Vorschriften nicht einhalten zu können, schalteten viele Firmen, Vereine und private Blogger ihre Onlineangebote einfach ab, obwohl oben genannte Hinweise schon längst für jeden Webseitenbetreiber ein Thema hätten sein sollen. So entschied der komplette Vereinsvorstand der Bewegungs- und Rehabilitationssportgemeinschaft Ingelheim, aufgrund der Rechtsunsicherheit und der drohenden Strafen, sein Amt zum 24. Mai niederzulegen. Die Tagesschau berichtete darüber.

Was hat sich nun wirklich geändert?

Es steht außer Frage, dass es Änderungen im Rahmen der Informationspflichten, Betroffenenrechte, des Auskunftsersuchens und der Meldefristen sowie generell der Transparenz im Umgang mit personenbezogenen Daten gibt. Viele Aspekte der DSGVO gilt es, in der Praxis noch zu erproben.

Abmahnwelle in Sicht?

Mit Ablauf der Übergangsfrist begann das Geschäft des einen oder anderen Abmahnanwalts, der im ersten Schritt Abmahnungsbeträge forderte, die der Abgemahnte ggf. bereit ist zu bezahlen. Dies kann teuer werden. Die Höhe der geforderten Unterlassungsansprüche führte allerdings dazu, dass viele Unternehmen den angesetzten Betrag „nicht einfach bezahlten", sondern ggf. durch eine vorab abgeschlossene Rechtsschutzversicherung Widerspruch einreichten. Je nach Perspektive ist dieses Vorgehen gut oder schlecht. Fakt ist allerdings, dass die Gerichte auf dem Gebiet „Abmahnungen wegen fehlender oder mangelhafter Datenschutzerklärung" erst durch monate- oder gar jahrelange Prozesse zu allgemeingültigen Urteilen kommen werden.

Was nehmen wir für die Zukunft mit?

Auf der Strecke blieb bei der „Panikmache" leider recht häufig der eigentliche Grundgedanke des Datenschutzes. Aus der falschen Annahme, Datenschutz sei eine Sache, die „mal eben so" erledigt werden könne, ergaben sich zahlreiche Geschäftsmodelle, die versuchten, die vorherrschende Unsicherheit für sich zu nutzen. Mein Appell: Konzentrieren Sie sich doch mal wieder auf das Wesentliche. ■

Nina Richard

CHECKLISTE DATENSCHUTZ*

- ✔ **Muss ich einen Datenschutzbeauftragten bestellen?**
- ✔ **Ist mein Datenschutzbeauftragter bei meiner zuständigen Aufsichtsbehörde gemeldet?**
- ✔ **Sind die Kontaktdaten meines Datenschutzbeauftragten auf meiner Webseite aufgeführt?**
- ✔ **Ist meine Webseite datenschutzrechtlich auf dem neusten Stand?**
- ✔ **Bin ich zur Erstellung einer Datenschutz-Folgenabschätzung verpflichtet?**
- ✔ **Habe ich ein Verzeichnis der Verarbeitungstätigkeiten?**
- ✔ **Existiert eine Datenschutzrichtlinie, die Aspekte wie Berechtigungen und Zugriffsrechte sowie Zuständigkeiten und die Sensibilisierung mit dem Thema beinhaltet?**
- ✔ **Sind Verträge und Formulare an die DSGVO angepasst?**
- ✔ **Besteht die Möglichkeit, den geforderten Betroffenenrechten (z. B. Informationspflicht, Auskunftsrecht, Löschung) nachzukommen?**
- ✔ **Sind die Verträge mit externen Dienstleistern entsprechend angepasst?**

* Auszug zu der Checkliste: Wie die Maßnahmen jeweils umzusetzen sind, ist vom Einzelfall abhängig. Lassen Sie sich von einem Experten unterstützen.

Leitfäden erleichtern die Erstellung konzepten im Gesundheitswesen

In Zusammenarbeit mit der Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (GMDS-AG DIG) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) hat das ZTG Zentrum für Telematik und Telemedizin einen Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen erarbeitet. Analog dazu und ergänzt um die Arbeitsgruppe „Datenschutz und IT-Sicherheit“ des Bundesverbandes Gesundheits-IT e. V. (bvitg) haben die Partner zudem einen Leitfaden für die Erstellung von IT-Sicherheitskonzepten im Gesundheitswesen entwickelt. Beide Dokumente sind kostenfrei zum Download verfügbar (www.ztg-nrw.de/beratung/).

von Datenschutz- und IT-Sicherheits-

Die Digitalisierung in der Gesundheitsversorgung gewinnt auch in Deutschland verstärkt an Dynamik. Datenschutz und die Sicherheit vor unbefugten Zugriffen haben höchste Priorität bei der Übertragung und Verarbeitung von Daten im Gesundheitswesen. Vor allem im Zuge der seit dem 25. Mai 2018 wirksamen Europäischen Datenschutzgrundverordnung (EU-DSGVO) und der damit verbundenen umfangreichen Nachweispflichten gewinnen Datenschutz- und IT-Sicherheitskonzepte erneute Aufmerksamkeit.

Schnell und sicher

Bisher gab es bei der Erstellung von Datenschutzkonzepten im Gesundheitswesen noch keinen Leitfaden mit einem standardisierten Vorgehen. Der Leitfaden für die Erstellung von Datenschutzkonzepten ermöglicht ein schnelles und sicheres Erstellen von Datenschutzkonzepten anhand einer Mustergliederung mit Hinweisen zu wichtigen Aspekten und einer Arbeitshilfe. Er beruht auf zahlreichen Rückmeldungen von Datenschutzexpertinnen und -experten. Er ist unter der Creative-Commons-Lizenz CC-BY-SA lizenziert und daher kostenfrei verfügbar. Das Vorgehen bei der Erstellung eines Datenschutzkonzeptes wird als Folge von fünf Einzelschritten erklärt. Anhand des ausführlich beschriebenen Step-by-Step-Prozesses können Datenschutzkonzepte schnell und unter Erfüllung höchster Sicherheitsanforderungen erstellt werden. Gezielte Fragen und Hinweise ergänzen den Arbeitsprozess.

> *Die elektronischen Patientendaten müssen manipulationssicher und vertraulich verarbeitet werden.*

Technischen Herausforderungen begegnen

Mit der zunehmenden Verbreitung und Relevanz von eHealth-Anwendungen steigen auch die Anforderungen hinsichtlich der IT-Sicherheit der eingesetzten informationstechnischen Verfahren: Die elektronischen Patientendaten müssen manipulationssicher und vertraulich verarbeitet werden, was sowohl die Nutzung in der Patientenbehandlung betrifft als auch den Austausch dieser Daten zwischen den verschiedenen Akteuren. Mithilfe eines IT-Sicherheitskonzeptes lässt sich ein systematisches Vorgehen etablieren, um sowohl den gesetzlichen Anforderungen als auch den sich schnell verändernden technischen Möglichkeiten und Herausforderungen angemessen zu begegnen.

Der Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes wendet sich im Speziellen an Einrichtungen, Institutionen und auch Organisationen des Gesundheitswesens – unabhängig davon, ob sie im Bereich der Gesundheitsversorgung oder Gesundheitsforschung tätig sind – und ermöglicht ein standardisiertes Erstellen von IT-Sicherheitskonzepten mit einer Schritt-für-Schritt-Anleitung und ausführlichen Hinweisen zur erfolgreichen Umsetzung. Er fungiert als eigenständige Ergänzung zum Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen. Beide Leitfäden sind kostenfrei verfügbar unter: **https://www.ztg-nrw.de/beratung/**. ■

Eric Wichterich

Dipl.-Inform. Med.
Eric Wichterich
Leiter Telematikdienste,
Datenschutz und IT-Sicherheit
e.wichterich@ztg-nrw.de

Das ZTG Zentrum für Telematik und Telemedizin (Bochum) ist ein herstellerunabhängiges eHealth-Kompetenzzentrum.

Ziel ist die Verbesserung der Gesundheitsversorgung auf Basis von Innovationen aus der Informations- und Kommunikationstechnologie.

ZTG koordiniert die Landesinitiative eGesundheit.nrw. Insbesondere berät sie über Datenschutz, Interoperabilität und Nutzerorientierung.
https://www.ztg-nrw.de/

Wie leben Sie Datenschutz und Informationssicherheit?
Fragen Sie Ihre Mitarbeiter.

Datenschutz und Informationssicherheit können nur so stark sein, wie die Kultur innerhalb der Einrichtung es zulässt. Jeder einzelne Mitarbeiter muss den Datenschutz in seinen Alltag integrieren und für den Umgang mit Daten und Informationstechnologien sensibilisiert werden. Nicht erst gesetzliche Anforderungen, wie die DSGVO, das IT-Sicherheitsgesetz oder die angekündigte ePrivacy-Verordnung, machen Datenschutz und Informationssicherheit zur Managementaufgabe. Die Beschäftigtenumfrage MaBIS gibt dem Management und Datenschutzbeauftragten ein Werkzeug zur Ist-Stand-Erhebung an die Hand.

Die Beschäftigtenbefragung MaBIS setzt dort an, wo die Beratung über Datenschutz und Informationssicherheit endet und Maßnahmen geplant werden sollen oder bereits umgesetzt wurden. Erste Recherchen ergaben, dass große Schwachstellen in diesem Kontext häufig Informationsdefizite bei einzelnen Mitarbeitern sind. Verantwortliche müssen wissen, inwieweit die Vorgaben zur Informationssicherheit und zum Datenschutz bei ihren Mitarbeitern angekommen sind und gelebt werden. Gleichzeitig ist zu berücksichtigen, wie die Einrichtung und das Management im Kontext der Informationssicherheit und des Datenschutzes von den Beschäftigten wahrgenommen werden: Inwieweit sind Informationssicherheit und Datenschutz in alle relevanten Unternehmensprozesse integriert?

Kurzinfo MaBIS

Die Beschäftigtenbefragung MaBIS ist eine Gemeinschaftsentwicklung von DATATREE und prolytics. Die Benchmarkstudie wird im vierten Quartal 2018 durchgeführt, Individualbefragungen können ab sofort beauftragt werden.

Welche Themen werden in der Beschäftigtenbefragung behandelt?

Um festzustellen, inwieweit Informationssicherheit und Datenschutz in der Einrichtung gelebt werden, ist es unerlässlich, alle Einflussfaktoren zu evaluieren. Häufig gehen diese Themen in ihrer Detailtiefe im Unternehmen weit über das hinaus, was der Mitarbeiter in seinem privaten Kontext erlebt. Dennoch spielt z. B. die private Einstellung zum Datenschutz eine große Rolle bei der Implementierung von Maßnahmen und Richtlinien im Unternehmen (Abbildung 1).

MaBIS ist als Onlinebefragung konzipiert, kann aber auch schriftlich durchgeführt werden, wenn die Mitarbeiter oder bestimmte Gruppen von Mitarbeitern über keinen adäquaten Rechnerzugang verfügen.

Benchmarking – wie schneidet das eigene Unternehmen im Vergleich zu anderen ab?

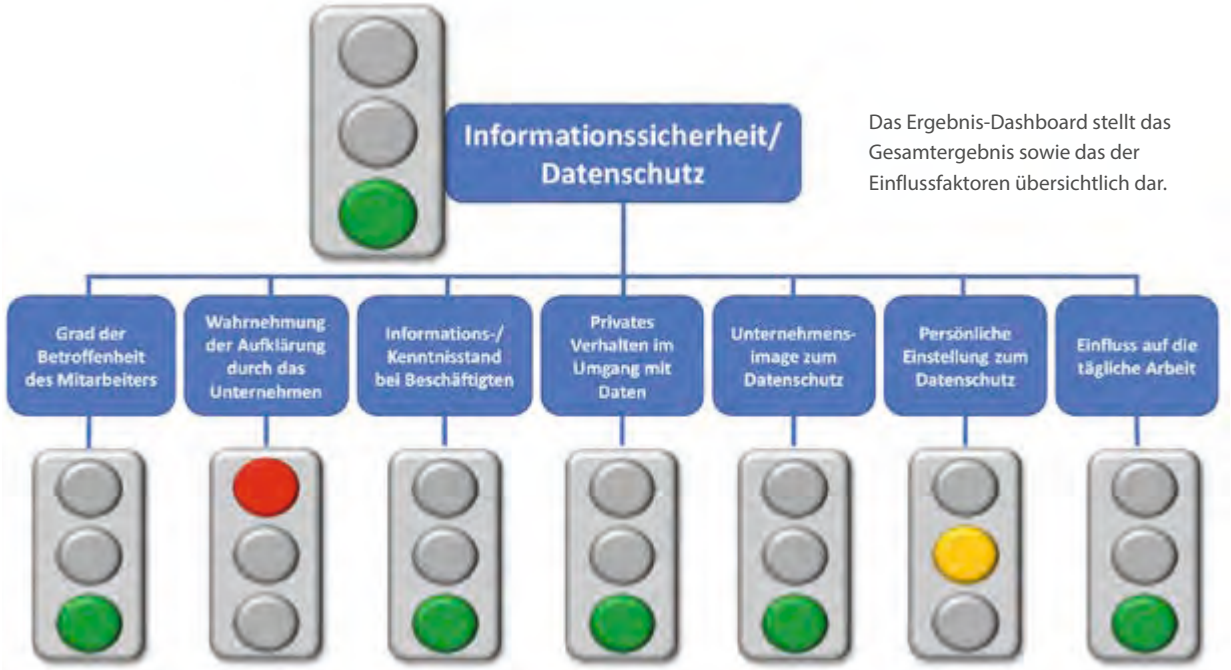
Für eine sinnvolle Einordnung der Ergebnisse der eigenen Einrichtung ist es hilfreich, einen

So vielfältig wie umfangreich: die Einflussfaktoren auf den Stand der Informationssicherheitskultur innerhalb Ihres Unternehmens

Michael Groß, Geschäftsführer prolytics

KURZPROFIL PROLYTICS

Seit der Gründung 1995 beschäftigt sich prolytics neben anderen Branchen vor allem mit den Fragestellungen des Gesundheitswesens, insbesondere im Rahmen von Gefährdungsbeurteilungen im Auftrag des WIdO (Wissenschaftliches Institut der Allgemeinen Ortskrankenkassen).



Das Ergebnis-Dashboard stellt das Gesamtergebnis sowie das der Einflussfaktoren übersichtlich dar.

validen Vergleichsmaßstab zu haben. Ein solcher Benchmark muss nicht nur das Gesundheitswesen, sondern alle Institutionen und Unternehmen in Deutschland beinhalten. Zur Ermittlung dieses Benchmarks wird eine bundesweite Onlinestudie mit einer Stichprobengröße von n = 5.000 Interviews durchgeführt, sodass neben repräsentativen Gesamtergebnissen auch aussagekräftige Benchmarks für unterschiedliche Differenzierungen (Branchengruppen, Unternehmensgrößen etc.) ausgewiesen werden können.

Wie werden Maßnahmen abgeleitet?

Zur Ergebnisdarstellung werden ein übersichtliches und leicht verständliches Ampelsystem eingesetzt und Indices berechnet. Die Geschäftsführung, der Datenschutzbeauftragte oder andere verantwortliche Mitarbeiter können sich einen schnellen Überblick über die Situation im Unternehmen insgesamt, aber auch über verschiedene Abteilungen verschaffen. Maßnahmen können somit direkt priorisiert und zielgenau implementiert werden.

Das hat MaBIS zu bieten

- Dokumentation des Erfüllungsgrades von Informationssicherheit und Datenschutz im Unternehmen
- Präzise Identifikation von Schwachstellen
- Zielgenaue Einleitung von Verbesserungsmaßnahmen
- Unterstützung bei der Gestaltung von Informationssicherheit und Datenschutz ■

Michael Groß

Qualitätssicherung oder Hackerspielerei?

Pentesting als Teil der Informationssicherheit

Live-Hacking, Pentesting, White- und Blackbox-Test – Begrifflichkeiten, die uns dank diverser Veranstaltungen im Gedächtnis geblieben sind. Existieren Unterschiede in den Verfahren oder wird ausschließlich im Vokabular differenziert? Wir gehen dem Ganzen auf den Grund.

Nach dem einen oder anderen Hackerangriff in den letzten zwei Jahren, mit dem sich die Öffentlichkeit auseinandersetzte, entwickelte sich gleichermaßen großer Respekt wie auch Interesse an dem mysteriösen Mann im Kapuzenpulli.

Begriffe wie Live-Hacking waren Teil von vielen Veranstaltungen zum Thema Sicherheit, bei denen mehr oder minder gute „Hacker" sich an explizit für diesen Fall vorbereiteten Systemen zu schaffen machten und aufzeigten, dass sie mit zwei Eingaben im Quellcode einer Website Benutzerdaten abgreifen konnten. Was auf den ersten Blick beeindruckt, wird beim zweiten Blick langweilig. Vielen „Live Hackern" scheint der Showeffekt wichtiger zu sein, als das Aufzeigen echter Gefahren. Beim zweiten Mal langweilte es mich, weil mir klar wurde, dass es sich hierbei nur um ein reißerisches Veranstaltungsformat handelte. Ich traf mich mit unserem Verantwortlichen für Informationssicherheit und wollte von ihm wissen, welche Technik hinter diesem Vorgehen steckt und ob es einen Mehrwert für die Informationssicherheit im Krankenhaus darstellen könnte.

Unser Verantwortlicher für Informationssicherheit hält hiervon wenig. „Oft ist es doch nur Angstmacherei mit inszenierten Fällen, die mit real auftretenden Situationen häufig wenig zu tun haben."

Die Testmethode, die hinter dieser „Showtechnik" steckt, sind die sogenannten Penetrationstests (kurz: Pentests), die Elemente innerhalb eines Netzwerks, von Softwaresystemen oder Webanwendungen testet. Es werden Werkzeuge und Angriffsmuster von Hackern nachgebildet.

Was kann getestet werden

Grundsätzlich kann jede IT-Anwendung und jedes zugrunde liegende Trägersystem getestet werden. Als Einstiegspunkte können beispielsweise genutzt werden:

- Web- und Datenbankserver
- Switches
- Fileserver
- Speichersysteme
- Clients
- drahtlose Netzwerke
- ... etc.

Innerhalb des Vorgehens unterscheidet man drei Arten von Pentests:

- Whitebox-Test
- Greybox-Test
- Blackbox-Test

Beim Whitebox-Test liegen dem Prüfer umfangreiche Informationen über die zu testenden Systeme vor. So werden vorab vom Auftraggeber IP-Adressen sowie eingesetzte Soft- und Hardware, Architekturdiagramme, Quellcode und weiterführende Informationen übermittelt, die einen ganzheitlichen Systemüberblick ermöglichen.

> *Der Pentester hat immer zu vermeiden, dass die zu prüfenden Systeme zu Schaden kommen.*

Bei dem sogenannten Blackbox-Test stehen lediglich Adressinformationen zur Verfügung. Diese Art von Test stellt die Simulation eines typischen Außentäters

dar, dem nur unvollständige Informationen vorliegen.

Zum Greybox-Test existieren verschiedene Definitionen am Markt und auch das Vorgehen und Verfahren zum Greybox-Test ist eine Grauzone, da nicht definiert ist, welche Informationen vorzuliegen haben. Genau das macht den Test aber so beliebt, da viele Auftraggeber über mangelnde Dokumentationen verfügen.

Welche Testart empfiehlt das BSI?

„Das BSI empfiehlt, grundsätzlich Whitebox-Tests durchzuführen, da bei einem Blackbox-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können. Es besteht die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt werden. Zusätzlich besteht bei einem Blackbox-Test ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen. Darüber hinaus ist der Aufwand bei einem Blackbox-Test wesentlich größer als bei einem Whitebox-Test. Den Prüfern sollten daher nach Möglichkeit alle für die Testdurchführung notwendigen Informationen über die zu testenden Systeme zur Verfügung gestellt werden." (BSI 2017)

Egal für welche Testart Sie sich entscheiden: Der Pentester hat immer zu vermeiden, dass die zu prüfenden Systeme zu Schaden kommen.

Der Pentester

Einen guten Penetrationstester auszuwählen, ist gar nicht so einfach. Dies liegt in einer Sache begründet: Das Geschäft des Testers lebt von Verschwiegenheit, sodass das Aufführen von Referenzen gegen seinen Ehrenkodex verstößt. Natürlich kann der Auftraggeber hierzu auch seine Zustimmung erteilt haben. Nichtsdestotrotz sollte der Prüfer Ihnen aber eine Aussage zu den Branchen, Testsystemen und Umfängen seiner Arbeit geben können. Ein guter Pentester arbeitet nicht nach Checklisten, sondern agiert flexibel gemäß der Anforderungen des zu testenden Systems. Checklisten können allerdings dem Auftraggeber als organisatorische Orientierung dienen – mehr aber auch nicht.

> *Das Geschäft des Testers lebt von Verschwiegenheit, sodass das Aufführen von Referenzen gegen seinen Ehrenkodex verstößt.*

Die hauseigene IT ist für diesen Job nicht geeignet. Die Frage nach dem Warum lässt sich einfach beantworten. Nur so ist die Unabhängigkeit zum Prüfprojekt gegeben. Zudem sollten Interessenkonflikte ausgeschlossen werden können.

Profilbildungsversuch

Der Tester ist nicht der Qualitätsbeauftragte für Ihre IT. Dennoch kann er ein sinnvoller Teil des Qualitätsmanagements sein.

- Frei von Interessenkonflikten
- Keine Abhängigkeitsverhältnisse
- Kann Qualitätssicherung nicht ersetzen (kann aber ein Teil davon sein)

Fachlich sieht die Empfehlung des BSI folgende Anforderungen vor:

- Der Tester sollte umfangreiche fachliche Kenntnisse haben. Werden Nachweise in den weiter unten angegebenen Bereichen vorgelegt, so kann von einer breiten fachlichen Qualifikation ausgegangen werden.
- Ohne die Vorlage von Zertifikaten sollte zunächst anhand des Prüfobjekts entschieden werden, welche Qualifikationen erforderlich sind. Ein erfolgreicher Prüfer im Webanwendungsbereich ist nicht zwangsläufig auch dafür geeignet, das IT-Sicherheitsgateway zu untersuchen.
- Wenn ein allgemeiner IS-Penetrationstest angestrebt wird, so sollten folgende Bereiche von den Prüfern beherrscht werden:
  - Systemadministration
  - Netzwerkprotokolle
  - Programmiersprachen
  - IT-Sicherheitsprodukte (IT-Sicherheitsgateways, Intrusion-Detection-Systeme etc.)
  - Anwendungssysteme
  - Netzkomponenten
- Es ist hilfreich, wenn ein Prüfer selbst schon im Bereich Systemadministration oder Programmierung gearbeitet hat, da er hierdurch Erfahrung mit allen möglichen Fehlerquellen mitbringt.
- Bei einer vertrauensvollen Person für IS-Penetrationstests, sind neben den technischen Kenntnissen weitere Fähigkeiten sehr wichtig. Ein Prüfer sollte folgende Qualitäten besitzen:
  - organisatorische Fähigkeiten
  - zielorientiertes Denken und Handeln
  - Überzeugungsfähigkeit
  - schnelle Auffassungsgabe
  - gesundes Urteilsvermögen
  - analytische Fähigkeiten
  - Teamfähigkeit
  - Belastbarkeit
  - Sachlichkeit insbesondere bei heiklen Sachverhalten
- Die aufgezählten Fähigkeiten lassen sich nicht einfach nachweisen. Bei der Beauftragung eines Prüfers muss sich die Institution daher bei diesen Punkten teilweise auf die eigene Intuition und die Erfahrungen mit dem Auftragnehmer verlassen. Einige Anhaltspunkte lassen sich jedoch auch aus den Angeboten herauslesen. Beispielsweise können anhand der Referenzen Rückschlüsse gezogen werden. Es ist aber auch möglich, dass der Anbieter keine Referenzen vorlegen kann, weil die geprüften Institutionen einer Nennung nicht zugestimmt haben. Gerade bei IT-Sicherheitstests nach erfolgreichen Angriffen herrscht eine größere Verschwiegenheit. Hierbei kann es für den Anbieter nützlich sein, sich bestätigen zu lassen, in welchen Branchen er gearbeitet hat und welche Unternehmensgröße die bereits getesteten Institutionen hatten. Wichtige Punkte sind die Unabhängigkeit und die Neutralität der Prüfer. Steht ein Prüfer in einem Abhängigkeitsverhältnis zu der getesteten Institution, so fehlt ihm die notwendige Unabhängigkeit, die für

> *Ein Prüfer muss die Möglichkeit haben, ohne Konsequenzen für sich, auch sehr negative Aspekte für die getestete Institution ansprechen zu können.*

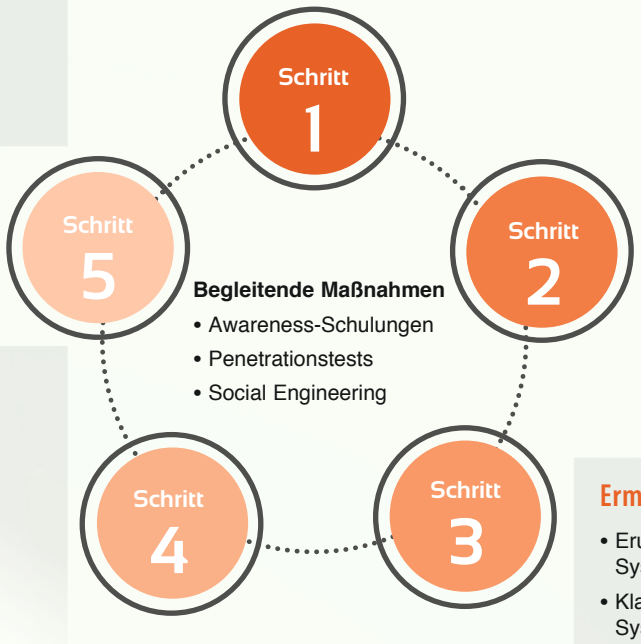
VORGEHENSBESCHREIBUNG ZUR EINFÜHRUNG IHRES INFORMATIONSSICHERHEITS-MANAGEMENT-SYSTEMS

Initiales Assessment

- Bestimmung des Scopes
- Interview/Workshop
- Zieldefinition
- Evaluierung der Verantwortlichkeiten
- Dokumentation und Aufbau eines Vorgehensmodells
- Definition weiterer Vorgehensweisen/Maßnahmen

Risikomanagement

- Planung und Durchführung von Maßnahmen
- Maßnahmentracking
- Durchführung von internen und externen Audits
- Akzeptanz des Restrisikos



Policy-Erstellung

- Zusichern von Management Attention
- Benennung ISB

Beschreibung des ISMS

- Strukturierung und Beschreibung der Prozesse des ISMS
- Dokumentation von relevanten Schritten

Maßnahmenabgleich

- Ausführliche Istanalyse nach bewährten Standards (z. B. ISO 27001/BSI Grundschutz)
- Risikoanalyse
- Maßnahmenableitung
- Handlungsempfehlungen
- Ergebnisdokumentation

Ermittlung des Schutzbedarfs

- Eruierung von genutzten Systemen und Diensten
- Klassifizierung und Bewertung von Systemen und Daten
- Darstellung potenzieller Risiken für die einzelnen Systeme und Dienste

jede Art von IT-Penetrationstest unerlässlich ist. Ein Prüfer muss die Möglichkeit haben, ohne Konsequenzen für sich, auch sehr negative Aspekte für die getestete Institution ansprechen zu können.

WANN IST EIN PENTEST DAS RICHTIGE FÜR SIE?
Wenn Sie als Unternehmen sich vor externen Angreifern schützen möchten und/oder bereits Opfer eines Anfriffs geworden sind.

Warum nicht einfach selbst machen

Das Internet ist voll von kommerziellen oder frei zugänglichen Tools. Einige Programme sind sehr speziell auf bestimmte Anwendungsfälle zugeschnitten. Ein Tester muss die Tools mit allen Einsatzgebieten kennen und sie selbst testen, bevor er diese einsetzt. Diese Dinge sollten Sie vorab vereinbaren:

- Nie ohne schriftlichen Auftrag testen
- VERTRAG! Ggf. muss auch der Hoster von Diensten mit einbezogen werden
- Rahmenbedingungen wie Prüfzeitraum, Prüfobjekt und Prüftiefe festlegen
- Kosten festlegen und was sonst noch zu erwarten ist, z. B. Präsentation vor dem Management, und die Mitwirkungspflichten
- Haftungsfreistellung
- Verschwiegenheitsvereinbarung
- Speichern von Daten (teilweise müssen Daten auch für den Bericht gespeichert werden)
- Datenschutz

Pentesting als Teil des Ganzen

Grundlegende Herausforderungen wie mangelnde Zuständigkeiten, Ressourcen und fehlendes Problembewusstsein machen Einrichtungen und Unternehmen anfällig für drohende Gefahren. Nur mit einem strukturierten Managementansatz können effektiv die eigentlichen Herausforderungen bewältigt werden.

Notwendig ist ein Managementsystem für Informationssicherheit, das im ersten Schritt eine grundlegende Basisorganisation rund um die Informationssicherheit aufbaut. Hierzu haben sich folgende Schritte bewährt:

1. Initiales Assessment
2. Policy-Erstellung/Beschreibung ISMS
3. Ermittlung des Schutzbedarfs
4. Maßnahmenabgleich
5. Risikomanagement

Aber auch begleitende Maßnahmen wie z. B. Penetrationstests. Der Penetrationstest bildet eine Maßnahme, die ihr volles Potenzial nur ausschöpfen kann, wenn sie in einen ganzheitlichen Ansatz eingebettet ist. ■

Nina Richard

„Mit verschlossenen Augen geht es nicht“

Im Interview mit Nenad Ljubetić

Die Ganzheitlichkeit der Informationssicherheit wird häufig unterschätzt. Deshalb wagen wir den Blick über den Tellerrand. Was kann das Gesundheitswesen von einem Chemielogistik-Dienstleister lernen?

Insellösungen, ineffiziente Budgetnutzung und im Worst Case das Verschließen der Augen von Verantwortlichen vor den eigentlichen Kernproblemen. Nicht nur bei den aktuell 120 Krankenhäusern, die die Anforderungen nach KRITIS bis 2019 umsetzen müssen, sondern auch bei jedem anderen Krankenhaus sollte das Thema auf der Agenda stehen. Um Fortschritte für die eigene Branche zu erzielen, ist es enorm wertvoll, einen Blick nach rechts und links zu werfen. Hinweg über den eigenen Tellerrand. Nur wer die Vielfalt von existierenden Ansätzen, Konzepten und Meinungen kennt, kann diese bewerten und sein Know-how weiter ausbauen, um wichtige Themen erfolgreich bei den richtigen Entscheidern zu positionieren. Der Austausch mit Spezialisten anderer Branchen ist durch nichts zu ersetzen.

Wir haben Nenad Ljubetić, Head of Business IT bei dem in Hürth ansässigen Chemielogistiker TALKE, zum Interview mit der ExperSite gebeten. Ein Interview über technologischen Fortschritt, menschliche Emotionen und die Norm ISO 27001.

*ExperSite: **Sie sind Head of Business IT bei der TALKE-Gruppe. Wie kann ich mir Ihren Aufgabenschwerpunkt vorstellen?***

Ljubetić: Ich verantworte die gesamte Wertschöpfungskette sämtlicher Anwendungssysteme bei TALKE. Hier seien beispielsweise diverse SAP-Systeme genannt, die sowohl in unseren logistischen als auch in den kaufmännischen Geschäftsfeldern eingesetzt werden. Darunter fallen ebenso Anwendungssysteme einer Reihe anderer Hersteller und Disziplinen.

Bei einem international tätigen Chemielogistik-Dienstleister hat das Thema Sicherheit oberste Priorität. Ist das ein Thema für den Betriebsrat, die Personalabteilung oder die IT-Abteilung?

Weder noch: Der Themenkomplex Sicherheit betrifft ausnahmslos alle. Der Schutz von Menschen und Umwelt nimmt eine fundamentale Bedeutung in unserem Unternehmen ein und bestimmt folglich unser verantwortungsvolles Handeln bei der Einhaltung von Sicherheitsanforderungen und Präventionsmaßnahmen.

Gilt dies auch für das Thema Informationssicherheit?

Selbstverständlich! Die Informationssicherheit wird als eine Teildisziplin unserer gesamten Sicherheitsstrategie interpretiert. In einem Umfeld, das geprägt ist von Bewegung, Wandel und Fortschritt, gewinnt sie tagtäglich enorm an Bedeutung. Praktisch betrachtet, bedeutet dies, dass die Informationssicherheit neben dem Schutz von Unternehmensassests, nicht etwa einem ein-

Nenad Ljubetić

ist als Head of Business IT bei dem Chemielogistik-Spezialisten TALKE verantwortlich für die Integration, Standardisierung und Automatisierung der Business-IT-Systemlandschaft und der umgebenden IT-Prozesse.

dimensionalem Selbstzweck dient, sondern vielmehr Ausdruck eines verantwortungsvollen Handelns innerhalb der Gesellschaft ist.

Im Gesundheitswesen wird häufig die Meinung vertreten, dass man Jahre hinter dem aktuellen Stand der Technik zurückliegt. Wie sehen Sie das und was leiten Sie daraus für die Informationssicherheit ab?

Dieser Eindruck mag in der Außenwahrnehmung verbreitet sein, unterstreichen kann ich ihn – nicht zuletzt aus meiner mehrjährigen Erfahrung als IT-Leiter eines Dienstleisters im Gesundheitswesen – nicht. Meine Begründung ist simpel und zugleich komplex: Informationssicherheit ist kein reines Technikthema. Vielmehr handelt es sich um einen ganzheitlichen Managementansatz, der Prozesse bündelt und sinnvoll lenkt. Hierzu gehören dann natürlich auch technische Maßnahmen. In der Regel beeinflusst – nicht entscheidet – der Modernitätsgrad von IT-Technik die Wirksamkeit von Schutzmaßnahmen. Vielmehr stellen die Kombination aus der unternehmensinternen Einstellung im Umgang mit Fragestellungen der Informationssicherheit und dem Reifegrad von Prozessen, aber auch Konzepte der Personalqualifikation eine elementare Basis dar, die stabil genug ist, ausgebaut und weiter optimiert zu werden. Der angemessene Technologie-Einsatz sollte meiner Ansicht nach „lediglich" einen flankierenden Charakter bei der Erreichung der Schutzziele besitzen.

Sie erwähnten einen ganzheitlichen Managementansatz. Kann das Thema Informationssicherheit hiermit strukturiert angegangen werden?

Strukturen und Prozessreife sind leider nicht käuflich. Zwar können Unternehmen Unterstützung mit ins Boot holen, um beispielsweise Prozesse zu analysieren und zu optimieren. Allerdings liegt es am Ende an der Unternehmenskultur, diese kontinuierlich zu verinnerlichen und (vor-)zuleben. Einen guten Ausgangspunkt für Verantwortliche für Informationssicherheit bieten diverse Kompendien, so beispielsweise der „Leitfaden für Informationssicherheit", herausgegeben vom BSI, der diverse Fragestellungen im Kontext der Informationssicherheit strukturiert und thematisiert. Die größte Herausforderung liegt meiner Erfahrung nach in der Verankerung der Maßnahmen im Unternehmen. Etabliert hat sich hier eine Reihe von Leitsätzen, beispielsweise Sicherheitsaspekte bereits frühzeitig im Rahmen von Projekt- und Änderungsvorhaben zu berücksichtigen, Sicherheitsrichtlinien aktuell zu halten, Verantwortlichkeiten zu benennen, die Ansprüche in die Organisation zu kommunizieren sowie die Wirksamkeit umgesetzter Maßnahmen regelmäßig zu überprüfen. Und: Motivation und Treiber sollte nicht der Handlungsdruck, sondern ein positives Selbstverständnis und eine chancenorientierte Einstellung zur Informationssicherheit sein.

Können Sie hier Best-Case-Beispiele nennen?

Naja, ein Leitfaden für den sicheren Umgang mit mobilen Endgeräten beispielsweise. Hier habe ich zwei Möglichkeiten, das Thema anzugehen. 1. Ich verfasse eine Leitlinie auf höchstem Fachniveau, unter Berücksichtigung von Juristen, den IT-Kollegen, dem Datenschutzbeauftragten und der Geschäftsführung. Dieses Dokument entspricht am Ende vermutlich den Ansprüchen aller Beteiligten. Das Problem: Ich habe meine eigentliche Zielgruppe übersehen – nämlich jeden einzelnen Mitarbeiter des Unternehmens. Sie werden diesen Leitfaden niemals lesen, geschweige denn, sich neben ihrer regulären Tätigkeit ausreichend Fachwissen aneignen können, um das Fachchinesisch verstehen zu können. Möglichkeit 2 hingegen: Ich sehe mich als Schnittstelle, bündle und übersetze den Leitfaden für Laien und setze mich mit der Unternehmenskommunikation an einen Tisch, um die emotionale Ansprache für unsere Mitarbeiter zu entwickeln.

Sollten bewährte Standards wie der BSI-Grundschutz/ISO 27001 Usus sein oder gibt es auch andere Möglichkeiten, das Thema Informationssicherheit anzugehen?

Obwohl sich IT-Grundschutz und ISO 27001 angenähert haben, empfehle ich zusätzlich den Schulterblick. Hier denke ich beispielsweise an das IT-Grundschutzkompendium, das Anforderungen konkreter ausgestaltet als in der ISO 27001. Eine Gliederung der Anforderungen in Basis, Standard und hoher Schutzbedarf sowie eine Klassifikation nach Muss, Soll und Kann helfen, Aufwände in der Umsetzung durch eine Anforderungsorientierung zu reduzieren. Darüber hinaus sind darin umfassende und hilfreiche Umsetzungshinweise mit entsprechenden Maßnahmenvorschlägen (analog ISO 27002) hinterlegt. Fundament beider Konzepte ist ein Risikomanagement, d. h. die konsequente und vorangehende Auseinandersetzung mit der Identifikation, der Bewertung und der Reduzierung von Sicherheitsrisiken.

Viele Verantwortliche beklagen, keine Ressourcen zur Verfügung gestellt zu bekommen. Muss es denn immer das große Budget sein?

Hier verfahre ich nach dem Prinzip: Erst die Botschaft und sich dann über die Mittel Gedanken machen. Ich rege an, Schutzbedarf und Mussmaßnahmen in den Vordergrund der Diskussion zu stellen und erst im Anschluss das benötigte Budget und ggf. weitere Rahmenvoraussetzungen zu ermitteln. Andernfalls besteht die Gefahr, dass die Anforderungen durch eine Budgetdiskussion verwässert und die eigentliche Zielsetzung in den Hintergrund gerät. Sollte das Budget tatsächlich nicht im benötigten Maß zur Verfügung stehen, empfehle ich, den Optionsspielraum durch alternative Ansätze zur Reduzierung der Sicherheitsrisiken zu erweitern.

Welchen Rat können Sie anderen Verantwortlichen für den Aufbau von IT-Sicherheitsmanagement-Systemen (ISMS) mit auf den Weg geben?

Der Aufbau eines ISMS ist ein komplexes und unternehmensweit wirkendes Thema und darf daher in zeitlicher, aber auch in kultureller Hinsicht nicht unterschätzt werden. Zur Realisierung des Informationsschutzes sind beispielsweise Unternehmensrichtlinien zu erstellen, geeignete Prozesse, Methoden, Verantwortlichkeiten und Ressourcen zu definieren und angemessen einzusetzen. Heißt: Die gesamte Organisation muss sensibilisiert und Ressourcen bereitgestellt werden, was zugegebenermaßen kein leichtes Unterfangen ist und eine fortlaufende Herausforderung darstellt. Alternativlos erscheint hier ein Ansatz, ausgehend von den Geschäftsprozessen die dazugehörigen Anwendungs- und Infrastrukturkomponenten gegenüberzustellen, die Informationswerte zu definieren und Risiken zu analysieren. Im Anschluss sollten Maßnahmen abgeleitet und bei Bedarf Verbesserungen umgesetzt werden. Nach meiner Erfahrung ist dies ein alternativloser Ansatz, der zeitintensiv ist, die Einbindung von Experten verlangt und keine isolierte Betrachtung von Beteiligten und Systemen zulässt. Und: Machen Sie sich keine Hoffnung, dass dieser Prozess irgendwann endet.

Herr Ljubetić, herzlichen Dank für Ihre Zeit!

TALKE zählt zu den international führenden Logistikdienstleistern für die chemische und die petrochemische Industrie. Kernkompetenzen des 1947 gegründeten Unternehmens sind der Transport, die Lagerung und der Umschlag gefährlicher und harmloser Stoffe aller Aggregatzustände. Darüber hinaus bietet der Logistikspezialist Beratung, Design und Implementierung entsprechender Strukturen, Prozesse und Anlagen an.

TALKE ist mit insgesamt mehr als 3.700 Mitarbeiterinnen und Mitarbeitern in Europa, dem Nahen Osten, Indien, China und den USA aktiv.

9. Goldene Regel: Kommunikator DSB

Die Anforderungen an den Datenschutzbeauftragten sind groß. Neben fachlichem Know-how hat er auch im Bereich der Sozialkompetenzen zu überzeugen.

Datenschutz ist mehr als ein gesetzlich gefordertes Thema, mit dem Sie sich auseinandersetzen sollten. Sie müssen sich mit der Benennung eines Datenschutzbeauftragten (DSB) und seinen Aufgaben der Unterrichtung, Beratung und Überwachung in Bezug auf datenschutzrechtliche Fragestellungen beschäftigen. Dazu gehört auch die Zusammenarbeit des DSB mit den Aufsichtsbehörden.

Wirklich erfolgreich kann Datenschutz nur sein, wenn dieser in die Unternehmenskultur integriert und somit „gelebt" wird. Mit diesen vier Tipps bleibt das Thema in der Unternehmenskommunikation präsent.

1. Bilden Sie eine Arbeitsgruppe oder Datenschutz Task Force

Damit Datenschutz ein Erfolgsthema in Ihrer Einrichtung werden kann, brauchen Sie Verbündete. Auch wenn es per Gesetz Verantwortliche für den Datenschutz gibt, muss auch jeder einzelne Mitarbeiter seine Aufgabe innerhalb des Gesamtkonstrukts verstehen. Nur durch ein engmaschiges Kontrollsystem können Probleme frühzeitig identifiziert und rechtzeitig Gegenmaßnahmen eingeleitet werden. Um das Thema erfolgreich in Ihrer Einrichtung zu kommunizieren, bedarf es der Zusammensetzung eines sinnvollen Projektteams. Dazu sollten gehören:

- Datenschutzbeauftragter
- Unternehmenskommunikation
- Geschäftsführung
- IT-Abteilung
- Medizinische Mitarbeiter

2. Kommunizieren mit Plan

Das Thema Kommunikation sollte Bestandteil Ihres Datenschutz-Management-Systems sein. Ein solches System besteht aus verschiedenen Bestandteilen, die alle Maßnahmen sowie ihre Implementierung und Kontrolle innerhalb der Organisation umfassen.

Die kommunikativen Prozesse sollten allerdings nicht willkürlich ablaufen, sondern entsprechend eines vorab entwickelten Kommunikationskonzepts gesteuert werden. Ein Kommunikationskonzept für den Datenschutz ist für Sie wie ein Fahrplan, an dem Sie sich orientieren können. Neben der Zielsetzung werden Dialoggruppen ermittelt, Textstile und konkrete Maßnahmen festgelegt.

3.Kommunizieren Sie zielgruppengerecht

Sie haben Ahnung von Ihrem Fach und brennen für Ihr Thema … gar keine Frage und das ist auch gut so. Allerdings geht es Ihren Kollegen und Mitarbeitern damit ggf. anders. Die Fachexpertise der übrigen Belegschaft liegt gemäß ihres Stellenprofils und ihrer Ausbildung aller Voraussicht nach in anderen Schwerpunkten als dem Datenschutz. Berücksichtigen Sie dies und halten Sie Ihre Kommunikation für den Laien verständlich.

4. Seien Sie Partner, nicht Verhinderer

Die Einhaltung von Datenschutzrichtlinien führt teilweise dazu, dass Projekte nicht, wie von den Initiatoren geplant, ohne Nachbesserung durchgewunken werden können. Das Ziel des DSB muss es sein, dass jeder Mitarbeiter bei der Initiierung eines jeden Projektes das Thema Datenschutz zumindest einmal bedacht hat. Wenn Sie dieses Ziel erreicht haben, achten Sie darauf, bei Problemen nicht als Verhinderer wahrgenommen zu werden. Besser: Machen Sie aus Problemen Chancen und gehen diese lösungsorientiert an.

PS: Nicht immer kann man alle Projektbeteiligten glücklich machen … das ist aber auch nicht Ihre Aufgabe. Sie haben mit Ihrer beratenden Tätigkeit die Aufgabe, auf Risiken hinzuweisen und Lösungsmöglichkeiten aufzuführen, die sich aus Art. 39 ergeben. ■

Nina Richard

HCM Academy

Krisenmanagement und Krisenkommunikation im Gesundheitswesen

22. November, Allianz Arena München

eine Veranstaltung von Health & Care Management

Programm

Dr. Christina Berndt,
investigative Journalistin, Süddeutsche Zeitung, Medizin und Wissen
„Die andere Seite – Skandale in Kliniken und Pflegeheimen aufdecken“

Monika Röther,
Geschäftsführerin, Klinikum Ingolstadt
„Wie leitet man ein Klinikum aus der Krise heraus? Dos and Don’ts aus der Praxis“

Dr. Tobias Weimer,
Fachanwalt für Medizinrecht, WEIMER | BORK
„Eine Reise durch das Strafrecht – was kann passieren im Falle des Falles?“

Johannes Lenz,
Head of Content, WhatsBroadcast
„Krisenkommunikation in sozialen Medien – Fluch oder Segen?“

Peter Höbel,
Geschäftsführer, crisadvice Unternehmensberatung
„Mit Kommunikation die Krise kompetent managen. Praxis vom Profi“

HIGHLIGHTS

- Meister ihres Fachs als Referenten
- spannende Themen mit konkretem Praxisbezug und interaktiven Elementen
- nachhaltiges Networking mit Experten und Profis
- aufregendes Rahmenprogramm in einmaliger Atmosphäre

Einführungsveranstaltung:
Speed-Dating der Teilnehmer

Tutorien:
Einzeldiskussion mit allen Referenten

Feldstudie:
Stadionführung und geselliger Ausklang

Weitere Informationen und Anmeldung unter: www.hcm-magazin.de/academy

FKT

Heilwesen Netzwerk RM eG

Datenschutz langweilt Sie?

Das geht auch anders! Mit Praxisnähe, Professionalität und Leidenschaft . Wir zeigen Ihnen wie!

Trotz gesetzlicher Bestimmungen und Anforderungen muss Datenschutz kein langweiliges Thema sein. Mit unserem Ziel Datenschutz lebbar zu gestalten, erfüllen wir die Bedürfnisse aller Interessenten – von der Geschäftsführung bis hin zum einzelnen Mitarbeiter: Datenschutz gesetzeskonform und spannend umgesetzt.

Datenschutz strukturiert aufbauen:

- ganzheitliches Datenschutz-Managementsystem
- modular aufgebaut
- gesetzliche Vorgaben erfüllen
- Datenschutz als Teil Ihrer Unternehmensphilosophie

MEDICA

Besuchen Sie uns auf der Medica!
Halle 15, Stand C05

DATATREE
YOUR COMPLIANCE PROVIDER

ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

DATATREE AG • Heubesstraße 10 • 40597 Düsseldorf
T +49 211 93190-700 • F +49 211 93190-799
office@datatree.eu • www.datatree.eu

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

Michael Groß, prolytics market research GmbH

Nenad Ljubetić, TALKE GmbH & Co KG

Eric Wichterich, ZTG GmbH

Die nächste Ausgabe erscheint im März 2019