Ausgabe 03| 2020

ExperSite

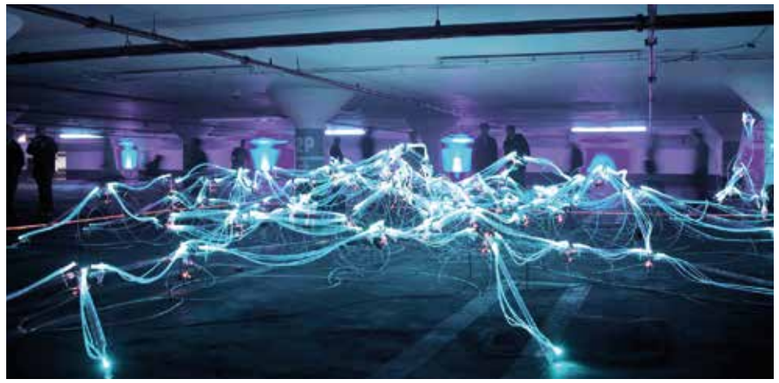
Das Magazin für Informationssicherheit und Datenschutz

10 Seiten zum **Krankenhaus-zukunftsgesetz**

PDSG, EU-U.S. Privacy Shield, Cookie Richtlinie, KHZG –

Licht am Ende des Tunnels?

Virtueller DSB-Lehrgang – ein Erfahrungsbericht 9



Das Patientendatenschutzgesetz ebnet den Weg für die elektronische Patientenakte 22

Das Privacy Shield wurde gekippt 4

Sicher Apps im Unternehmen verwenden 7

DATATREE
YOUR COMPLIANCE PROVIDER

www.datatree.eu

Lassen Sie uns eine kurze Reise wagen

Stellen Sie sich vor, Sie stehen in der Szenerie unseres Magazintitels. Ebendiese Szenerie, die uns als Redaktionsteam in den Sinn kam, als wir versuchten, das Jahr, welches nun hinter uns liegt, zu umschreiben. Wir gehen durch eine Tür und stehen in einem Raum. Umdrehen können wir uns nicht. Unser Blick macht sich mit seiner Umgebung vertraut. Wir sehen etliche weitere Räume, die sich dem uns umgebenden Raum anschließen, verbunden mit einem Durchgang. Was sich in den einzelnen vor uns liegenden Räumlichkeiten befindet, wissen wir nicht.

Für uns alle war es ein Jahr voller Unbekannter. Und so betraten wir Raum für Raum, ohne zu wissen, was uns nach unserem Eintritt in diesem Raum erwartet.

Wir wurden gefordert. Jeder für sich. Beruflich, wie privat. Aber auch für die Themen Informationssicherheit und Datenschutz war es ein unglaublich bedeutendes Jahr. Denn nie zuvor wurde ebenso die Praktikabilität und Sicherheit von Lösungen von allen Seiten gleichermaßen gefordert – ach ja, und schnell musste es gehen. Wo es möglich war, wurden Home-Office Regelungen und Remote-Lösungen geschaffen, was wiederum Sicherheitskonzepte, Policies und existierende Prozesse (falls vorhanden) auf die Probe gestellt hat. Und als wäre das nicht genug, wurde die Datenübertragung in die USA zu einem rechtlich heiß diskutierten Thema. Privacy-Shield adé!

Und immer dann, wenn man dachte, man könne kurz durchatmen, betrat man den nächsten Raum. Plötzlich kam der Gesetzgeber zum Zuge und verabschiedete noch das ein oder andere Gesetz. Das Patientendaten-Schutz-Gesetz oder auch das Krankenhauszukunftsgesetz waren nicht die einzigen Themen, die uns in 2020 beschäftigten. Gerade lässt sich hierzu aber nur sagen: Auch 2021 bleibt spannend.

Und trotzdem ist es da. Das Licht am Ende des Tunnels. Die Zeit, in der wir uns alle einmal zum Durchatmen zwingen und uns bewusst machen sollten, was wir in diesem Jahr geschafft haben. Unsere kleinen und großen Erfolge feiern. In diesem Sinne möchte ich mich für die Loyalität und das regelmäßige Feedback unserer Leserschaft bedanken! Auch ein großes Dankeschön geht an das komplette DATATREE-Team, das redaktionell und grafisch immer mit viel Herzblut agiert und dieses Magazin erst zu dem macht, was es ist.

„Das Licht am Ende des Tunnels“

Ich freue mich auf ein gemeinsames 2021 mit Ihnen!

N. Richard

Ihre Nina Richard
(Redaktionsleitung)

Privacy Shield adé – und nun?

Das EU-U.S. Privacy Shield ist inzwischen Vergangenheit. Seitdem herrscht gerade unter Datenschutzbeauftragten eines: Verunsicherung. Jedes Unternehmen, das über Kunden verfügt, jede Behörde, die Bürgerdaten bearbeitet, und jede Institution, die personenbezogene Daten elektronisch mit einem Transfer in die USA verarbeitet, befindet sich in einem rechtlichen Konflikt. Was also tun?

Text: Jörg Fecke

Sichere Drittstaaten: Diese Länder zählen in Sachen Datenschutz für die EU-Kommission dazu.

1. **Andorra**
2. **Argentinien**
3. **Färöer**
4. **Guernsey**
5. **Isle of Man**
6. **Israel**
7. **Japan**
8. **Jersey**
9. **Kanada** (nur kommerzielle Organsisationen)
10. **Neuseeland**
11. **Schweiz**
12. **Uruguay**

Seit dem 16. Juli 2020 steht die Datenschutzwelt Kopf. Der Europäische Gerichtshof kippte nach jahrelangem Rechtsstreit zwischen der EU-Kommission und dem österreichischen Datenschutzaktivisten Max Schrems das EU-U.S. Privacy Shield. Damit fehlt vom einen auf den anderen Tag die rechtliche Grundlage für den Datenaustausch zwischen den USA und der Europäischen Union. Wieso? Während das US-Recht vorsieht, dass Behörden umfassenden Zugriff auf Daten von US- und Nicht-US-Bürgern erhalten, garantiert EU-Recht seinen Bürgern einen vergleichsweise hohen Schutz vor eben solchen Zugriffen. Man kann nicht beides haben – soweit so klar.

Was soll ich als Datenschutzbeauftragter in meinem Unternehmen jetzt anstoßen? Da gehen, wenig überraschend, die Meinungen weit auseinander. Während zum Beispiel die Berliner Datenschutzbeauftragte Maja Smoltczyk fordert, „umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln“, sehen andere weniger Handlungsbedarf und berufen sich auf Standardvertragsklauseln.

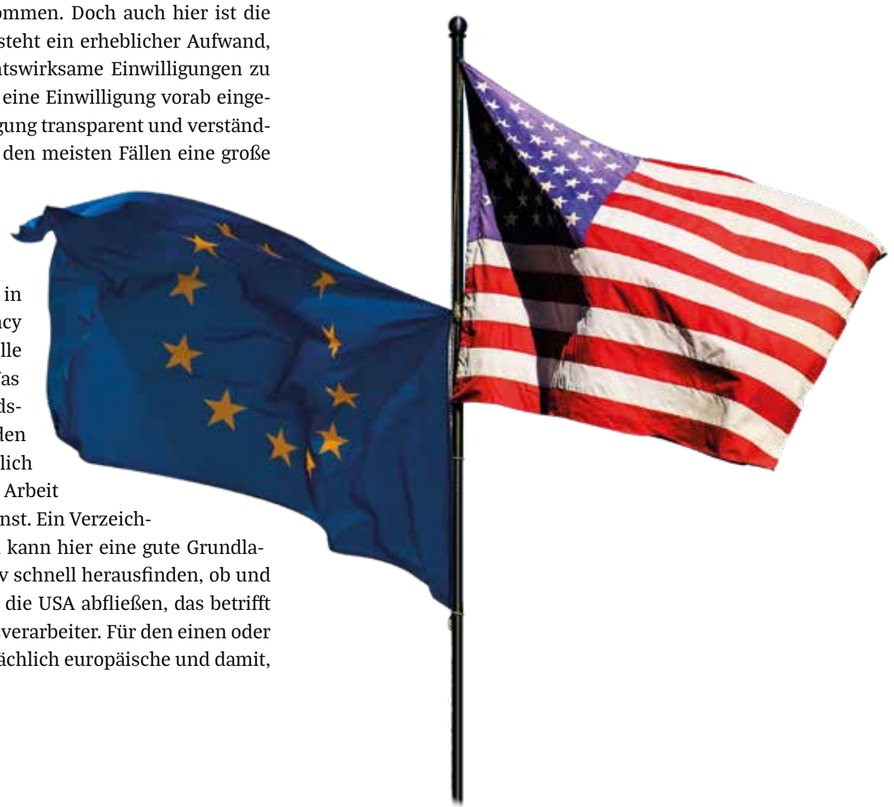
> Das Urteil zwingt Datenschutzbeauftragte zum Handeln

Diese hat der Europäische Gerichtshof nicht per se für nichtig erklärt. Im Gegenteil: Die Klauseln dürfen weiter genutzt werden. Allerdings mit einer Einschränkung: Die Nutzer der Standardvertragsklauseln müssen prüfen, ob die Rechte betroffener Personen auch im jeweiligen Drittland vergleichbar gut geschützt sind wie in der Europäischen Union. Die Standardvertragsklauseln sind damit also keine schnelle und einfache Lösung des Problems, beziehungsweise werden nicht dauerhaft Bestand haben. Auf Dienstleister aus den USA zu verzichten ist allerdings unrealistisch. Zahlreiche Dienstleister sind alternativlos. Es gibt keine ernstzunehmenden europäischen Lösungen für elementare EDV-Anwendungen wie MS-Office. Eine Firmenhandyflotte ohne Android, Apple oder Microsoft ist in den Augen des ein oder anderen vielleicht wünschenswert, aber schlicht nicht umsetzbar.

Die schlechteste Option ist einfach so zu tun, als ob einen das Urteil nicht betrifft. Es betrifft uns alle. Eine Übergangsfrist ist entfallen. Max Schrems hat inzwischen eine NGO gegründet. Sein Ziel: Beschwerde über Firmen, die zum Beispiel weiter Google Analytics nutzen, bei den jeweiligen Datenschutzbehörden einzureichen. Schrems möchte dabei vor allen Dingen den Schutz seiner ganz persönlichen Daten hervorheben. Das ist inzwischen in über 100 Fällen geschehen. Man darf gespannt sein. Nach der aktuellen Rechtsprechung bleibt den Datenschutzbeauftragten nicht allzu viel Ermessensspielraum. Der EuGH betont, dass Aufsichtsbehörden verpflichtet sind, unzulässige Datenabflüsse zu untersagen.

Die Zeit drängt

Datenschutzbeauftragten mag die Einwilligung als Mittel zur Rechtssicherheit in den Sinn kommen. Doch auch hier ist die Lage kompliziert. Einerseits entsteht ein erheblicher Aufwand, um für die jeweiligen Fälle rechtswirksame Einwilligungen zu formulieren. Andererseits muss eine Einwilligung vorab eingeholt werden. Dass diese Einwilligung transparent und verständlich formuliert sein muss, ist in den meisten Fällen eine große Herausforderung.



Die eine richtige Strategie existiert im Moment schlicht nicht. Auch wenn die EU-Kommission in Verhandlungen an einem Privacy Shield 2.0 arbeitet, eine schnelle Lösung ist nicht absehbar. Was hilft, ist eine individuelle Bestandsaufnahme. Das bedeutet für jeden Datenschutzbeauftragten natürlich Arbeit. Die gute Nachricht: die Arbeit der letzten Jahre war nicht umsonst. Ein Verzeichnis der Verarbeitungstätigkeiten kann hier eine gute Grundlage bilden. Damit lässt sich relativ schnell herausfinden, ob und wie personenbezogene Daten in die USA abfließen, das betrifft selbstverständlich auch Auftragsverarbeiter. Für den einen oder anderen Prozess lassen sich tatsächlich europäische und damit, in dieser Hinsicht, DSGVO-konforme finden. In anderen Fällen kann man aber auf die Großen aus dem Silicon Valley nicht verzichten. Außerdem sollte die Möglichkeit verschiedener technischer Maßnahmen in den Fokus rücken. Mit Ende-zu-Ende Verschlüsselung oder in Europa gehosteten Servern lässt sich das Sicherheitsniveau und damit auch das Datenschutzniveau erheblich erhöhen. Wichtiges Mittel der nachgewiesenen Maßnahmen ist übrigens eine saubere Dokumentation.

Panik ist kein guter Begleiter

Wer diese oder ähnliche Maßnahmen ergreift, braucht sich keine allzu großen Sorgen machen. //

Mögliche technische Maßnahmen:

- Ende-zu-Ende Transportverschlüsselung
- E-Mail-Verschlüsselung
- in der Europäischen Union gehostete Server
- Einführung von 2-Faktor-Authentifizierung
- gespeicherte Daten verschlüsseln

Der 8 Schritte-App-Check

Die Nutzung von mobilen Endgeräten bringt für Datenschützer vielfältige Herausforderungen mit sich. Insbesondere zur Bereitstellung von Basisfunktionen auf diesen Geräten sind mobile Applikationen erforderlich. Vor allem bei Meeting-Apps und Messenger-Diensten kommt es immer wieder zu Verunsicherungen, welche ohne großes Datenschutz-Risiko genutzt werden können und welche nicht. Zur Gewährleistung von Qualitätsstandards innerhalb der unternehmensinternen Datenschutz-Richtlinien bedarf es einheitlicher Regelungen für mobile Applikationen, denn Datenschutz kommt häufig noch viel zu kurz.

Text: Annika Raab

Grundlagen als Datenschutzverantwortliche immer im Blick haben

Privacy by Design und Privacy by Default sind zwei Begrifflichkeiten, die seit der DSGVO gesetzlich gefordert sind. Mit Privacy by Design ist gemeint, dass der Datenschutz durch das Ergreifen technischer und organisatorischer Maßnahmen (TOMs) unterstützt wird. Privacy by Default dagegen bedeutet, dass die Grundeinstellungen einer Applikation oder Webseite so gewählt sein müssen, dass ein Nutzer nicht aktiv gegen die Verarbeitung seiner Daten widersprechen muss, sondern nur dann tätig werden muss, wenn er dieser zustimmen möchte.

Um die gesetzlich geforderten Einstellungen in mobilen Applikationen bewerten zu können, benötigt man als Datenschutzverantwortlicher ein grundsätzliches Verständnis von personenbezogenen Daten, die Applikationen erheben können. Personenbezogene Daten betreffen natürliche Personen und können diese identifizierbar machen. Zu diesen Daten gehören neben dem eigenen Namen und Kreditkartennummern auch Daten für biometrische Erkennungsverfahren und Standortdaten. Selbst die IP-Adresse, die auf eine bestimmte Person zurückzuführen ist und daher eine ähnliche Funktion einnimmt wie eine physische Adresse, gehört zu den personenbezogenen Daten. Auch Gerätenummern, die auf eine Person schließen lassen, und Audiodaten, wie etwa Sprachnachrichten, fallen in diese kritische Kategorie.

Personenbezogene Daten

Außerdem gibt es besondere Kategorien personenbezogener Daten, zu denen unter anderem Gesundheitsdaten, die ethnische Herkunft oder die Zugehörigkeit zu einer Gewerkschaft zählen. Diese besonderen Kategorien dürfen allerdings nur in absoluten Ausnahmefällen verarbeitet werden.

Sie als App-Betreiber sind grundsätzlich für die Erhebung und Verarbeitung der Daten verantwortlich. In der DSGVO werden Dienstleister jedoch mit in die Verantwortung genommen.
Zur grundlegenden Überprüfung sollten Sie für Ihre sich im Einsatz befindlichen mobilen Applikationen einen Fragenkatalog zur Prüfung der Datenschutzkonformität erstellen. Wir liefern Ihnen hierfür eine erste Orientierung:

Verantwortlichkeiten

ERSTE ORIENTIERUNG FÜR IHREN FRAGENKATALOG

1. **Deckblatt erstellen!**
Dort notieren Sie alle wichtigen Fakten wie die Funktionen der App, die geprüfte Version, das Prüfdatum und den Prüfer. So können Sie zeitsparend auf einen Blick erkennen, um welche Applikation es sich handelt, mit welchen Funktionen sie den Arbeitsalltag erleichtern soll und wer die Prüfung der Anwendung übernommen hat.

2. **Sind die Mitarbeiter darüber aufgeklärt, welche mobilen Applikationen sie im Unternehmen nutzen dürfen?**
Mit dieser Maßnahme verringern Sie den Einsatz möglicher Schad-Software durch unwissende Mitarbeiter in Ihrem Unternehmen signifikant. Außerdem können Sie bei firmeneigenen Geräten der Installation einer neuen App eine Anfrage bei der IT-Abteilung voraussetzen.

3. **Welchen Nutzungszweck hat die App innerhalb des Unternehmens?**
So lassen sich schnell überflüssige Anwendungen erkennen, wenn eine andere Applikation bereits die Hauptfunktion der neuen Anwendung erfüllt.

4. **Welche personenbezogenen Daten werden erhoben?**
Mit diesem Schritt haben Sie einen Überblick darüber, welche Daten Ihre Mitarbeiter bei der Verwendung der App preisgeben müssen und ob die Datenerhebung konform mit Ihren Datenschutzstandards ist.

5. **Welche Tracking-Methoden (z.B. Cookies) werden durch den App-Anbieter eingesetzt?**
Auch dieser Punkt dient dem Überblick darüber, welche Daten erfasst werden und ob die Applikation datenschutzkonform eingesetzt werden kann.

6. **Welche Berechtigungen erfordert die App zur Nutzung?**
Viele Applikationen erfordern beim ersten Öffnen die Berechtigung, auf andere Apps, den Standort oder die Fotos zugreifen zu dürfen. Mit diesem Punkt der Checkliste haben Sie den Überblick über die erforderlichen Berechtigungen - und welche davon wirklich notwendig und datenschutzkonform sind.

7. **Welche Art der Verschlüsselung wird angewandt?**
Die Verschlüsselung ist ein wichtiger Faktor für die datenschutzkonforme Verwendung einer Applikation. Je besser die Verschlüsselung, desto schwerer haben es mögliche Eindringlinge, an die Daten Ihrer Mitarbeiter zu kommen.

8. **Werden durch den Anbieter ausreichend sichere Passwörter erzwungen?**
Der Mensch ist ein Gewohnheitstier - es kann anstrengend sein, sich immer wieder neue Passwörter merken zu müssen. Daher gibt es immer noch zahlreiche Menschen, die einfache Passwörter wie 12345 benutzen. Wenn die Applikation solche einfachen Kombinationen nicht zulässt, müssen Ihre Mitarbeiter bei der Passwortwahl kreativ werden - und das Sicherheitslevel steigt enorm. Damit Sie sich nicht alle Passwörter merken müssen, gibt es übrigens auch einige sichere Passwortmanager.

Ein Erfahrungsbericht

2020 steht unter keinem guten Stern für Präsenzveranstaltungen. Die DATATREE Akademie hat aus der Not eine Tugend gemacht. Die Weiterbildung zum zertifizierten Datenschutzbeauftragten findet inzwischen komplett virtuell statt. Ob das funktioniert? Wir haben die Teilnehmer gefragt.

Text: Nina Richard

Im August ist wieder unser Lehrgang zum/zur Datenschutzbeauftragten an den Start gegangen. Aber eine Sache war dieses Mal anders: Es war unser erster Lehrgang in diesem Umfang, den wir komplett online durchgeführt haben. Auch für die Teilnehmer war das Format Neuland. Über fünf Wochen lernten sie jeden Freitag per Videokonferenz die wichtigsten Werkzeuge eines Datenschutzbeauftragten kennen und diese in der Praxis einzusetzen. Die Dozenten: Unsere DATATREE-Experten für Datenschutz und Informationssicherheit.

Sowohl blutige Anfänger als auch Datenschutzbeauftragte mit einigen Vorkenntnissen haben gemeinsam an dem Lehrgang teilgenommen. Durch diese Konstellation sind interessante Diskussionen aufgekommen, die sogar teilweise auch bei den Dozenten für neue Erkenntnisse sorgten. Nach jedem theoretischen Part hieß es dann: Learning by Doing, indem die Teilnehmer aktiv mitwirkten und zum Beispiel ein Verzeichnis von Verarbeitungstätigkeiten erstellen sollten.
In dem Lehrgang wurden verschiedene Themen wie die allgemeinen Tätigkeitsfelder eines Datenschutzbeauftragten, die Auftragsverarbeitung, technisch-organisatorische Maßnahmen und Informationssicherheit genauer behandelt. Jedes Thema wurde von einem anderen Berater aus der Praxis vermittelt, was den gesamten Lehrgang aufgelockert hat.

Einige Teilnehmer berichten über ihre Erfahrungen, die sie in unserem Lehrgang machen konnten:

Exper*Site*: *Inwiefern hat der Lehrgang Ihre Sichtweise auf einige Datenschutzthemen geändert?*

Dudziak: Meine Sichtweise zum Themenfeld Datenschutz hat sich wesentlich verändert. Ich höre und beobachte intensiver die Belange Datenschutz, nicht nur im dienstlichen Bereich, auch in meinem persönlichen Bereich. Ich hinterfrage immer wieder: was möchte ich Dritten von mir preisgeben, was sollen Dritte von mir wissen, wie gehen Dritte mit meinen persönlichen Daten um...

Schlegel: Ja, ich habe gelernt, dass es immer schwierig ist, IT-Sicherheit und Datenschutz richtig zu trennen und zu bearbeiten. Der DSB muss die Einstellung der IT kontrollieren (z.B. Rollenverteilung, Zugriffsrechte usw.), darf aber dabei nicht die Firma „lahmlegen".

Raab: Der Lehrgang hat meine Sichtweise auf den Datenschutz sehr verändert. Ich wusste zwar vorher schon, dass überall personenbezogene Daten gesammelt werden, aber welches Ausmaß das Ganze hat und vor allem wie ich damit korrekt umgehen kann, habe ich in erster Linie durch diesen Lehrgang gelernt.

Exper*Site*: *Jetzt haben Sie das Zertifikat in der Tasche. Was haben Sie für Ihre Zukunft geplant?*

Dudziak: Für die Zukunft möchte ich das Fundament an Informationen und Grundlagen aus dem Kurs in meinem Arbeitsalltag umsetzen. Ich kann meine Aufgaben, denke ich, fachlich gerechter umsetzten. Zumindest habe ich einen Pool, in dem ich Hilfestellungen suchen und finden kann.

Schlegel: Ich arbeite als freiberuflicher Datenschutzbeauftragter. Die Kursinhalte sind für mich eine richtig gute Grundlage um mit Kompetenz Kunden und Kooperationspartner zu gewinnen.

Raab: Ich versuche nun in allen Lebensbereichen das Gelernte so gut es geht umzusetzen - sowohl im beruflichen Kontext als auch im privaten. Ich schaue mir bei jedem Webseiten-Besuch die Cookie-Einstellungen an und versuche auch im Bekanntenkreis Interesse am Thema Datenschutz zu wecken.

Exper*Site*: *Stellen Sie sich vor, Sie hätten einen Wunsch frei: Was würden Sie sich in Bezug auf Ihr Berufsfeld Datenschutz wünschen?*

Dudziak: Alle Beteiligten sollten sensibler mit dem Thema Datenschutz umgehen. In der heutigen digitalen Zeit werden so viele persönliche Daten preisgegeben, ohne Wissen oder mangels Nachfrage, die ich als Person nicht von mir preisgeben möchte. Kollegen in den Krankenhäusern würde ich empfehlen, sich einfach mal in Flure, Wartebereiche oder Anmeldungen zu setzen und zuzuhören. Was man da so alles mitbekommt von persönlichen Daten!!! Aktiver Datenschutz ist ein Thema für uns alle.

Schlegel: Ich würde mir mehr Anerkennung und einen höheren Stellenwert des Datenschutzbeauftragten bzw. Datenschutzberaters wünschen.

Raab: Ich würde mir wünschen, dass es weltweit einheitliche Richtlinien gibt, an denen man sich im Bereich Datenschutz orientieren kann und so Streitigkeiten oder Ungereimtheiten vermeiden kann. Damit wären unser aller Daten wesentlich besser geschützt und das Thema Datenschutz wäre vielleicht auch bei vielen nicht mehr so negativ behaftet, wie es ja leider noch allzu häufig vorkommt. //

LUDGER DUDZIAK

ist Datenschutzkoordinator am Katholischen Klinikum Essen und gleichzeitig in der dortigen Stabsstelle Qualitätsmanagement Pflege tätig.

SVEN SCHLEGEL

ist freiberuflicher Referent, Dozent und Berater zu den Themen Daten- und Arbeitsschutz.

ANNIKA RAAB

unterstützt die DATATREE AG seit September 2020 in der Marketing-Abteilung.

Krankenhauszukunftsgesetz, Cookie Richtlinie, Patientendatenschutzgesetz

Die Vielzahl an verabschiedeten Gesetzen der vergangenen Monate hat großen Einfluss für uns als Bürger, Unternehmer oder Patient. Das betrifft uns schon jetzt, aber besonders in Hinblick auf unsere Zukunft.

Text: Jörg Fecke

Das Krankenhauszukunftsgesetz ist in vielerlei Hinsicht ein Meilenstein. Mit über 4 Milliarden Euro fließt eine erhebliche Summe an Steuergeldern in die Krankenhaus-Infrastruktur. Auch hier steht die Digitalisierung im Fokus. Allein 15% der Fördersumme sind für die Stärkung der Informationssicherheit vorgesehen. Dabei bieten sich hier für Kliniken Fördermöglichkeiten, um gesetzlich vorgeschriebene Standards zu erfüllen. Diese, wie zum Beispiel ein Informationssicherheitsmanagementsystem für Nicht-KRITIS-Einrichtungen, sind ab 2022 vom Gesetzgeber verpflichtend.

Die Cookie-Richtlinie stellt sich nach wie vor als Herausforderung dar: Seitenbetreiber müssen sich über kurz oder lang mit dem Gedanken anfreunden, dass ein Tracking - wie im Moment noch weit verbreitet - mehr Nach- als Vorteile bringt. Das aktuell stark genutzte Consent Management ist in vielen Fällen mangelhaft implementiert – Bußgelder drohen.

Optimistisch kann die Gesundheitsbranche auf die nächsten Monate blicken. Das Patientendaten-Schutz-Gesetz ist verabschiedet und in Kraft getreten. Damit ist eine wichtige Grundlage für die elektronische Datenverarbeitung - und zwar DSGVO-konform - im Gesundheitswesen geschaffen worden. Die Chancen, dass die elektronische Patientenakte, dieses Wunschkind der vergangenen 16 Jahre, nun wirklich kommt, standen noch nie besser. //

Ein Gesetz der Möglichkeiten

Der Bundestag hat am 18. September 2020 Geschichte geschrieben. Mit der Verabschiedung des Krankenhauszukunftsgesetzes nimmt der Bund erstmals seit Jahrzehnten Geld in die Hand um signifikant in die Krankenhausinfrastruktur des Landes zu investieren.

Text: Jörg Fecke

Viel Geld für viele Themenfelder

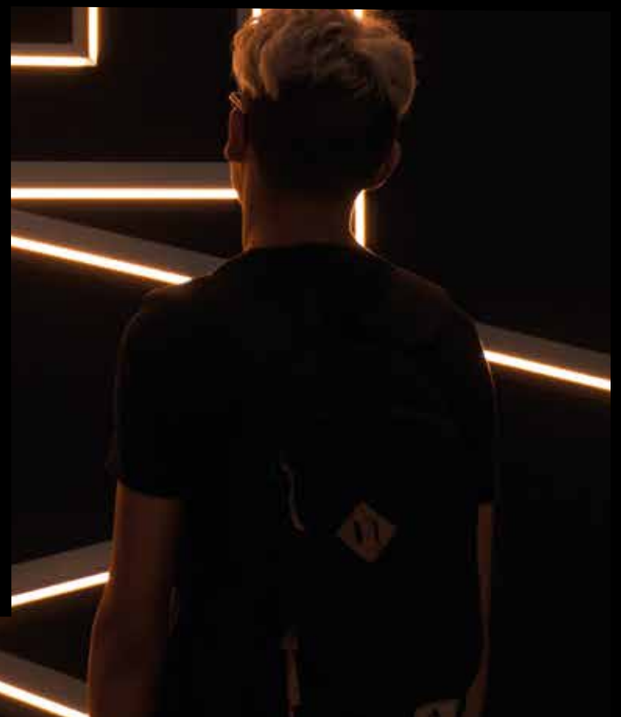
Mit der Verabschiedung des Krankenhauszukunftsgesetzes fließen insgesamt über 4 Milliarden Euro in die Modernisierung der Krankenhausinfrastruktur Deutschlands. „Damit wird 2021 ein Jahr, in dem so viele Investitionsmittel insgesamt für Krankenhäuser zur Verfügung stehen werden, wie nie zuvor“, erklärte Bundesgesundheitsminister Jens Spahn (CDU). Die dringend notwendige Maßnahme umfasst dabei Investitionen in Patientenportale, elektronische Dokumentation von Pflege- und Behandlungsleistungen, digitales Medikationsmanagement, sektorenübergreifende telemedizinische Infrastrukturen und nicht zuletzt die IT- und Informationssicherheit. Hier ergibt sich in der Förderfähigkeit eine besondere Situation. KRITIS-Häuser erhalten die Förderung über den Krankenhausstrukturfonds, alle anderen Häuser über den Krankenhauszukunftsfonds. Gerade die vergangenen Monate haben gezeigt, dass ohne gestärkte Informationssicherheit Krankenhäuser schon jetzt vor großen Herausforderungen stehen.

Wie genau Förderung beantragen?

Das Gesetz ist beschlossen, die Förderkriterien sind inzwischen definiert. Wichtig für die einzelnen Krankenhäuser ist schließlich der eigentliche Betrag, mit dem man kalkulieren kann. Die 3 Mrd. Euro des Bundes werden nach dem Königsteiner Schlüssel auf die Länder verteilt. 1,3 Mrd. Euro steuern die Bundesländer selbst bei. Daraus ergeben sich Fördersummen pro Krankenhaus von circa 1,7 bis 2,5 Mio. Euro. Die Frist für Förderanträge endet zum 31.12.2021. Realistisch ist eine Förderung bis September 2021, die Länder werden aller Voraussicht nach von Ihrem Recht auf dreimonatige Antragsbearbeitung Gebrauch machen.

Investition in IT-Sicherheit – wichtiges Kriterium für erfolgreiche Förderung

Die Vorbereitung für einen Förderantrag kann dennoch nicht schnell genug beginnen. Die Förderung ist an Voraussetzungen geknüpft, die eine hohe Komplexität und einen erheblichen Planungsbedarf voraussetzen. Darüber hinaus müssen mindestens 15% der Fördersumme in die Stärkung der IT-Sicherheit fließen – gerne beraten wir hier, um so einen positiven Förderantrag zu ermöglichen. //



Optimale Förderung mit dem Krankenhauszukunftsgesetz

Ein wesentlicher Betrag des Krankenhauszukunftsfonds soll in die Krankenhaus-IT fließen und hier auch ein höheres Sicherheitslevel ermöglichen. Beispiele aus der jüngsten Vergangenheit zeigen, dass hier erheblicher Handlungsbedarf besteht. Rund um die Beantragung der Förderung tun sich viele Fragen auf, die Hendrik Riedel zu beantworten weiß.

Text: Nina Richard

Welche Bedeutung hat Ihrer Meinung nach das Krankenhauszukunftsgesetz?

Das Krankenhauszukunftsgesetz (KHZG) ist richtig angewendet eine der größten Chancen sich als Krankenhaus mit einer gezielten Digitalisierungsoffensive zukunftsfähig aufzustellen. Es gilt aktuell aber auch die Grundprämisse: Digitalisiere oder zahle. Kliniken, die keine Digitalisierungsprozesse nach dem KHZG und auf Basis der Telematikinfrastruktur vorweisen können, kostet dies ab 2025 bis zu zwei Prozent Abschlag auf die Abrechnung aller voll- und teilstationären Fälle. Dies verstärkt das „Sanktionsszenario“, das bereits mit dem Verpassen der Frist für die technische Anbindung an die Telematikinfrastruktur zum 31.12.2020 verbunden ist. Der Krankenhauszukunftsfonds ist somit ein Krankenhausdigitalisierungsfonds, der neben der Steigerung der Versorgungsqualität die Nutzung der Anwendungen der Telematikinfrastruktur als Ziel hat und damit unter anderem den Einsatz der TI-Applikationen im Alltag der Ärzte, Apotheker und Patienten mit etablieren soll.

Das KHZG bietet dabei den Kliniken die Chance, sich über Digitalisierungsmaßnahmen stärker, leistungsfähiger und bedarfsgerechter aufzustellen, so dass eine bedarfsgerechte und zukunftsfähige Versorgung sichergestellt wird. Dabei sollten die Kliniken darauf achten, dass sie eine technische und organisatorische Infrastruktur aufbauen, die eine nachhaltige Innovations- und Transformationsfähigkeit etablieren. Denn niemand kennt die Zukunft und damit die Anforderungen von morgen.

HENDRIK RIEDEL

ist Geschäftsführer der Digital Avantgarde GmbH. Dank seiner langjährigen Berufserfahrung in der IT- und Dienstleistungsbranche verfügt er über zahlreiche Kenntnisse in medizinischer IT, Produktmanagement, Corporate Governance und anderen Geschäftsstrategien. Er ist Dipl-Wirtsch.-Ing. im Bereich Wirtschaftsingenieurwesen Maschinenbau.

Wer profitiert von der Förderung?

Mit dem KHZG sollen dabei Investitionen der Kliniken in verschiedenen Bereichen gefördert werden, darunter sind Bereiche, wie moderne Notfallkapazitäten, patientenzentrierte Mehrwertdienste, Ablauforganisation, Kommunikation, Telemedizin oder die gezielte Stärkung regionaler Versorgungsstrukturen.
Ein weiteres Schlüsselziel der Fördermaßnahmen ist laut Bundesgesundheitsministerium (BMG) die Vernetzung. Die Zeit der Insellösungen soll beendet werden. Dabei gehe es um die regionale Zusammenarbeit, aber auch um die interne und externe Vernetzung der Kliniken.
Ein wichtiger Schwerpunkt sei darüber hinaus die IT-Sicherheit, in die mindestens 15 Prozent der Fördergelder fließen müssen.
Des Weiteren fordert das BMG die Kliniken auf, sich schon frühzeitig mit den Fördermöglichkeiten auseinanderzusetzen, damit Digitalprojekte zügig angegangen werden können. So dürfen schon alle Projekte gefördert werden, die seit 02. September 2020 durchgeführt worden sind. Die Förderung erfolgt über die Länder. Anträge können bis Ende 2021 beim Bundesamt für soziale Sicherung (BAS) gestellt werden.
Für eine bedarfsgerechte, zukunftsfähige Versorgung brauchen wir starke, leistungsfähige und bedarfsgerechte Kliniken, die im Gesamten digital und technisch anschlussfähig sind.

„Wir brauchen leistungsfähige und bedarfsgerechte Kliniken."

Welche Leistungen werden gefördert?

Die Fördervorhaben sollen das Vorhaben „Zukunftsprogramm Krankenhäuser" umsetzen, wonach Verbesserungen hin zu einer moderneren und besseren investiven Ausstattung der Krankenhäuser durch eine Förderung moderner Notfallkapazitäten, einer besseren digitalen Infrastruktur, der IT- und Cybersicherheit sowie eine Stärkung regionaler Versorgungsstrukturen erreicht werden sollen.
Die spezifischen Fördertatbestände orientieren sich an der im Koalitionsbeschluss vom 3. Juni 2020 enthaltenen Aufzählung.
Hiermit soll jedoch keine thematische Abgrenzung voneinander verstanden oder aufgezeigt werden. Vielmehr greifen die Modernisierung und Digitalisierung der verschiedenen Bereiche ineinander, überschneiden sich, bauen aufeinander auf und ergänzen sich logisch und umfassen auch die digitale Barrierefreiheit.

„Wir haben eine Digitalisierungslandkarte mit förderfähigen Maßnahmen entwickelt."

Wir haben hierzu eine Digitalisierungslandkarte entwickelt, die exemplarisch 11 förderfähige Maßnahmen in ganzheitlichen Digitalisierungsprojekten abbildet.

Wie genau kann ich mir diese Digitalisierungslandkarte vorstellen?

Die Digitalisierungslandkarte vereint die EMRAM Logik mit dem ganzheitlichen Ansatz des KHZG. Sie zeigt auf, wie die elf förderfähigen Vorhaben aufeinander aufbauen und orchestriert werden, so dass eine nachhaltige Innovations- und Transformationsfähigkeit im Rahmen der Telematikinfrastruktur gewährleistet wird und so der Zusammenhang zwischen der internen Transformation zur Stärkung der regionalen Versorgungsstrukturen und -services deutlich wird. Die Digitalisierungslandkarte orientiert sich an einem typischen Ablauf eines stationären Krankenhausaufenthalts einer Patientin oder eines Patienten und sollen Aspekte aus den Teilprozessen „Aufnahme", „Behandlung" und „Entlassung" fördern. Die digitalen Services werden so gewählt, dass sie gezielt dazu beitragen, den Digitalisierungsgrad in den Krankenhäusern zu erhöhen, indem sie interoperabel in die Gesamt-IT-Struktur einzubetten sind. Hierdurch kann und soll eine stärkere Binnendigitalisierung angestoßen werden. Gleichzeitig soll sich ein unmittelbarer Nutzen für Patientinnen und Patienten entfalten können und gezielt die Versorgungsqualität erhöht werden. Das bedeutet zugleich, dass damit auch nicht-digitale Komponenten (z. B. der Notfallmedizin) gefördert werden. Mit den Fördertatbeständen werden keine neuen Rechtsgrundlagen für einen Datenaustausch geschaffen. Vielmehr soll ein rechtlich bereits gestatteter Datenaustausch lediglich digitalisiert werden.

„Ein weites Feld von Themen der Digitalisierung ist förderfähig."

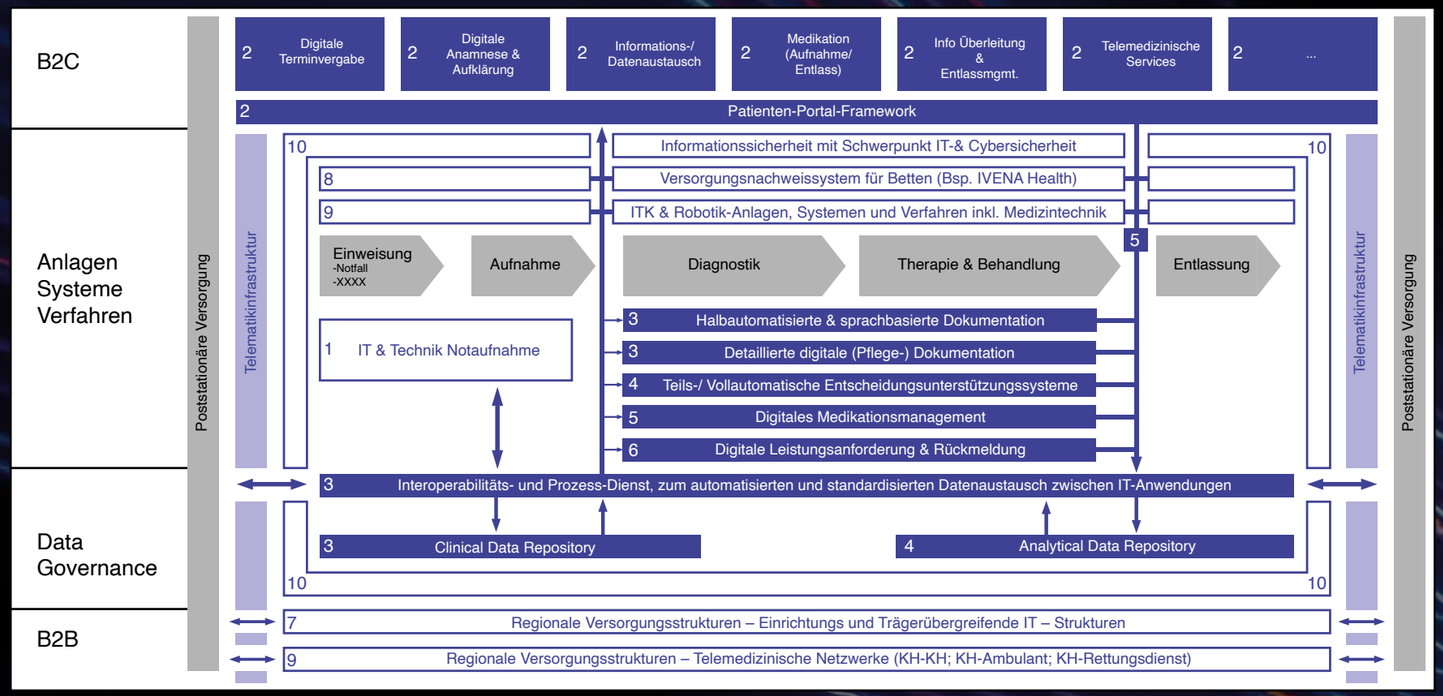
Krankenhäuser können nach § 19 des Krankenhauszukunftsgesetzes (KHZG) für die unten aufgeführten Vorhaben Anträge stellen und somit weitreichend profitieren. Die förderfähigen Vorhaben umfassen ein weites Feld von Themen der Digitalisierung in der Patientenversorgung.

Und Sie unterstützen Krankenhäuser auf der gesamten Prozessebene?

Ja genau. Hierzu haben wir den Digital-Avantgarde-Navigator entwickelt, ein Referenz- und Verfahrensmodell zur ganzheitlichen Digitalisierung von Krankenhäusern. Die Digital Avantgarde GmbH arbeitet neben den oben aufgeführten elf Primär-Themen auch die relevanten Sekundär-Projekte so aus, dass für den Förderträger deutlich wird, welche weiteren Maßnahmen im Krankenhaus das Erreichen der mehrwertstiftenden Nutzungsziele nachhaltig sichern und was diese förderungsfähigen Maßnahmen kosten.

Wie sollten Einrichtungen jetzt vorgehen? Sprich, gibt es Aspekte, über die man sich im Vorfeld Gedanken machen müsste?

Von Seiten der Krankenhäuser ist jetzt eine Qualitäts- und Digitalisierungsoffensive für notwendig. Das bedeutet, dass sie sich frühzeitig mit der Informationseinholung beschäftigen. Wir stellen unseren Kunden hierzu beispielsweise ein Whitepaper mit allen notwendigen Informationen zur Verfügung – und passen diese praktisch tagesaktuell an. Darüber hinaus bieten wir kostenlose Informationsveranstaltungen an, bei denen wir alle offenen Fragen beantworten und Möglichkeiten besprechen. //



Informationssicherheit – Förderung für ohnehin vorgeschriebene Umsetzung

Mindestens 15 Prozent eines jeden Fördervorhabens des Krankenhauszukunftsgesetzes sollen in die Informationssicherheit der jeweiligen Fördervorhaben fließen. Darüber hinaus sind Krankenhäuser, die Nicht-KRITIS-Einrichtungen sind, verpflichtet, ein Managementsystem für Informationssicherheit aufzubauen. Hierzu bleibt den Häusern gemäß §75 c SGB V ein Jahr Zeit; je nach Größe der Krankenhäuser ist das sportlich – aber nicht unmöglich.

Text: Nina Richard

Mit dem Ziel einer moderneren und besseren investiven Ausstattung der Krankenhäuser wird der Informationssicherheit in zukünftigen Förderprojekten eine erhebliche Rolle zugesprochen. Denn nicht nur die Förderung von technischen Komponenten, sondern auch nicht-digitale Komponenten, wie gezielte Maßnahmen zur Entwicklung und Stärkung des Regelbetriebes innerhalb von Krisenzeiten, machen auch Maßnahmen zur Awarenesssteigerung zum integralen Bestandteil der Investitionen. Konkret heißt es in den Förderrichtlinien:

„Hinsichtlich der Maßnahmen zur Gewährleistung der Informationssicherheit im Krankenhaus ist § 75c SGB V zu berücksichtigen und die ab dem 1. Januar 2022 geltenden Anforderungen grundsätzlich bei der Förderung nach §14a KHG anzuwenden. Es sind durchgehend entsprechende Maßnahmen zur Sicherstellung von der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von betroffenen Informationen zu etablieren."

In §75c SGB V wird hier konkret, dass ab dem 01. Januar 2022 Krankenhäuser dazu verpflichtet sind „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit (...) sowie deren Prozesse zu treffen." Zu erfüllen sind diese nach den branchenspezifischen Sicherheitsstandards B3S für alle Krankenhäuser, die nicht als Kritische Infrastruktur gelten.
Da bei allen nach dem KHZG geförderten Digitalisierungsprojekten mindestens 15 % des Fördervolumens für Maßnahmen der Informationssicherheit zu verwenden sind, können die gesetzlichen Anforderungen nach §75c SGB V mit Mitteln des KHZG gefördert werden. Dies gilt ausdrücklich nur für Nicht-KRITIS Häuser, da diese für die Umsetzung der KRITIS-Anforderungen den Krankenhausstrukturfond 2.0 nutzen können. Die Verbesserung der IT-Sicherheit hat der Bund 2019 als neuen Fördertatbestand in den Krankenhausstrukturfonds aufgenommen. Für die aktuelle Förderperiode 2019-2024 stehen beim Amt für Soziale Sicherung nun nicht mehr 500 Millionen, wie in der ersten Förderperiode, sondern insgesamt 750 Millionen Euro zur Verfügung.

Die wichtigsten Eckdaten zum Krankenhauszukunftsgesetz im Überblick

- Krankenhauszukunftsfonds = 3 Mrd. € (Bund)
- Kofinanzierung durch das jeweilige Land oder den Träger bis zu 1,3 Mrd. €
- Die meisten Bundesländer haben die Kofinanzierung der Bundesförderung fest eingeplant
- Maximal 10% der Mittel für Vorhaben an Hochschulkliniken
- Digitalisierungsvorhaben Nr. 2-6 geknüpft an Voraussetzungen (u. a. Interoperabilität ePA)
- Mind. 15% des Vorhabens für IT-Sicherheit
- Antragsfrist für die Länder bis 31. Dezember 2021

Informationssicherheit – Fördertatbestand 10: IT-Sicherheit (§19 Abs. 1 Satz 1 Nr. 10 KHSFV)

Ziel des Fördertatbestandes 10 ist die Verbesserung der IT- bzw. Cybersicherheit in Krankenhäusern, die nicht zu den kritischen Infrastrukturen gehören, sowie in Hochschulkliniken. Maßnahmen zur Verbesserung der Informations- bzw. Cybersicherheit sind bei diesen Krankenhäusern bisher von der Förderung nach dem Krankenhausstrukturfonds ausgeschlossen.

Auch in Krankenhäusern, die nicht zur kritischen Infrastruktur gehören, führt der zunehmende Grad der Digitalisierung zu steigenden Anforderungen bei der Informations- bzw. Cybersicherheit, der eine Berücksichtigung im Rahmen des Fördertatbestandes 10 dringend anzeigt.

Um eine optimale Versorgung der Patientinnen und Patienten zu gewährleisten und den Krankenhausbetrieb so effizient wie möglich zu gestalten, ist der Einsatz von zu Teilen hochkomplexen IT-Systemen notwendig und nicht mehr wegzudenken. Durch die zunehmende Vernetzung verschiedener Systeme und Komponenten steigen jedoch auch die Risiken hinsichtlich der Auswirkungen, die mit einem Ausfall oder der Beeinträchtigung ebendieser Systeme verbunden sind, im gleichen Maße. Zeitgleich werden die Angriffsflächen der IT- und Internettechnologien zunehmend vielfältiger und deutlich größer. Diesen muss durch geeignete Maßnahmen entgegengewirkt werden. Hierbei ist sowohl die Sicherheit der IT-Systeme als auch der dabei verarbeiteten Patientendaten in der Gesundheitsversorgung von höchster Bedeutung. Eine Vermeidung von Störungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse muss sichergestellt sein.

Gleiches gilt für die Authentizität der Daten. Nur so kann die Patientensicherheit und Behandlungseffektivität sowie die Funktionsfähigkeit des Krankenhaues aufrechterhalten und geschützt werden.

Informations- und Cybersicherheit sind die notwendigen Bedingungen für die fortschreitende Digitalisierung in den Kliniken. Dies kann durch ein geeignetes Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 oder BSI IT-Grundschutz gesteuert und überwacht sowie insbesondere durch die Umsetzung des Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus vollständig gewährleistet werden.

Förderfähigkeit von Informationssicherheit

Funktionale Anforderungen

Die im Folgenden skizzierten Anforderungen und darin exemplarisch dargestellten Sicherheitssysteme werden nicht solitär innerhalb eines der Bereiche Prävention, Detektion, Mitigation, Response oder Awareness eingesetzt, sodass eine Anwendung mehrere Bereiche abdecken kann.

Förderfähige Vorhaben zur Verbesserung der IT-bzw. Cybersicherheit müssen:

- die **Prävention** von Informationssicherheits-Vorfällen (u.a. Systeme zur Zonierung von Netzwerken, Next Generation Firewalls, sichere Authentisierungssysteme, Micro-Virtualisierung/Sandbox-Systeme, Schnittstellen-Kontrolle, Intrusion Prevention Systeme; Network Access Control, Schwachstellenscanner, Softwareversionsmanagement, Datenschleusen, Datendioden, VPN-Systeme, verschlüsselte Datenübertragung, verschlüsselte mobile Datenträger, ISMS)

oder

- die **Detektion** von Informationssicherheits-Vorfällen (u.a. Security Operation Center, Log Management Systeme, Security Information Event Management Systeme, Intrusion Detection Systeme, lokaler Schadsoftwareschutz mit zentraler Steuerung, Schadsoftwareschutz in Mailsystemen bzw. bei Mailtransport),

oder

- die **Mitigation** von Informationssicherheits-Vorfällen (u.a. automatisierte Backup-Systeme, lokaler Schadsoftwareschutz mit zentraler Steuerung)

oder

- die **Steigerung** und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen bzw. der Bedeutung von IT-/Cybersicherheit (u.a. regelmäßige Risikoanalysen, Schulungsmaßnahmen, Informationskampagnen, Awareness-Messungen)

oder

- eine **Kombination** davon zum Ziel haben.

Förderfähige Vorhaben zur Verbesserung der Informations- bzw. Cybersicherheit können Cloud- und KI gestützte Verfahren zur Erkennung von Angriffen als Gegenstand haben.

Informationssicherheit nachhaltig aufbauen

Der Aufbau eines ISMS bezeichnet bezeichnet den ganzheitlichen prozessorientierten Managementansatz zur Etablierung von Informationssicherheit innerhalb eines Krankenhauses. Innerhalb dieser Ganzheitlichkeit lässt sich das Vorgehen zum Aufbau eines ISMS in nachfolgenden Stufen darstellen:

STUFE 1:
RISIKO-ASSESSMENT
Innerhalb des initialen Risiko-Assessments geht es um die eigentliche Bedarfsermittlung innerhalb einer Einrichtung. Es handelt sich um eine Betrachtung der existierenden Verfahren zum Erhalt der Werte und Assets innerhalb der Organisation anhand von anerkannten Best-Practice Verfahren, wie z.B. der ISO 27001 Norm, spezifisch anhand des B3S-Standards. Das Ziel ist die Dokumentation des Soll-Ist-Standes, die Identifikation und Bewertung daraus abgeleiteter Risiken sowie die Priorisierung bzw. Empfehlung weiterer Handlungsschritte. Nur so können tatsächliche Bedarfe und Kosten für die Förderungen klar benannt werden.

STUFE 2:
AUFBAU EINES ISMS
Der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) ist nichts, was „mal eben" oder „nebenbei" zu erledigen ist. Der vom Gesetzgeber geforderte Zeitraum von einem Jahr ist mehr als knapp bemessen, und umso wichtiger ist ein strukturiertes Vorgehen für den Aufbau eines Informationssicherheitsmanagementsystems. Konkret unterstützen wir beim Aufbau einer geeigneten internen Organisation für Informationssicherheit und der Implementation eines ISMS. Dies geschieht auf Basis der Best-Practice-Standards, wie beispielsweise ISO/IEC 27001 Norm oder dem spezifischen B3S Standard. Die Tätigkeit umfasst den Aufbau und die Evaluation der mit dem ISMS eingeführten Prozesse und Vorgehensweisen.

STUFE 3:
ISB
Ergänzend oder alternativ zu Stufe zwei kann Stufe drei genau die richtige für Sie sein. Je nach Aufbau Ihrer Organisation ist es notwendig bzw. sinnvoll einen sogenannten ISB (Informationssicherheitsbeauftragten) zu bestellen. Dieser ist dann verantwortliche für den Aufbau und Erhalt des in Stufe 2 aufgeführten ISMS.

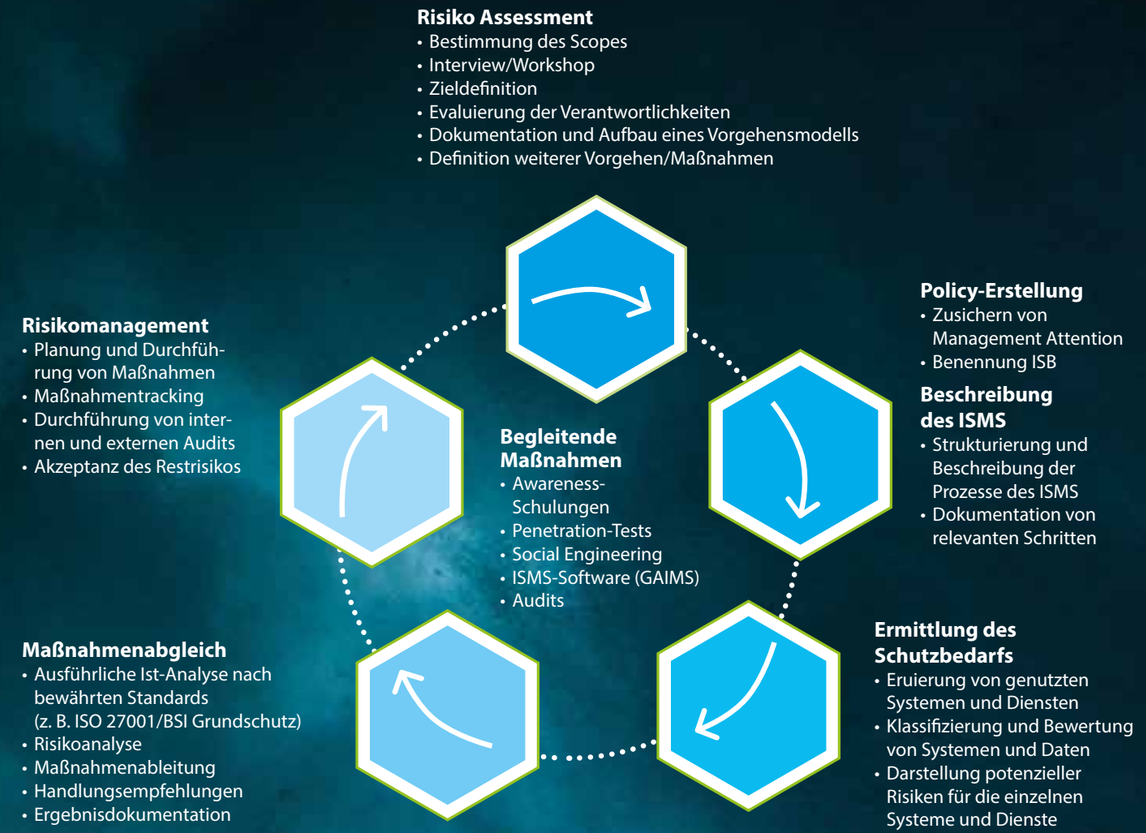
STUFE 4:
BEGLEITENDE MASSNAHMEN
Die nachfolgenden Dienstleistungen sind als begleitende Maßnahmen zu sehen:

Audits:
Planung und Durchführung von Informationssicherheits-Audits in der Organisation des Auftraggebers gehören auch zu unserem Portfolio. Die Dokumentation und Zusammenfassung der Abweichungen werden dann in einem Management-Bericht mit Bewertung möglicher Risiken festgehalten.

Awarenessmaßnahmen:
Maßnahmen, die von der klassischen Schulung vor Ort oder remote, über herkömmliche Learning-Management-Systeme, zu Feuerwehrübungen, Social-Engineering und weiteren Maßnahmen dieser Art reichen, sind äußerst wichtiger Bestandteil der nachhaltigen Informationssicherheit. //

Informationssicherheitsmanagementsystem aufbauen und stetig anpassen

Der Aufbau eines ISMS ist ein umfangreiches Projekt, welches durch stetige Anpassung und Optimierung auf- und ausgebaut wird.



Endlich! Sie ist da, die elektronische Patientenakte

Langsam, aber sicher kommt das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur. Es wird auch höchste Zeit, wir sind spät dran – ***ein Kommentar***

Text: Prof. Dr. Thomas Jäschke

Im Sommer hat der Bundestag das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, besser bekannt als Patientendaten-Schutz-Gesetz (PDSG), beschlossen. Inzwischen hat auch der Bundesrat das PDSG passieren lassen. Wir befinden uns damit auf der Zielgeraden eines langen, teilweise mühsamen und um so wichtigeren Weges hin zu einem digitalisierten Gesundheitswesen. Das PDSG ist gesetzliche Voraussetzung für die elektronische Patientenakte (ePA). Doch damit allein ist es nicht getan.

Im Vergleich zu vielen europäischen Nachbarn sind wir spät dran. Nach wie vor wird hierzulande eine Unmenge an Daten wie Befunde, Röntgenbilder oder Arztbriefe analog und dezentral gespeichert. Das ist in vielerlei Hinsicht ineffizient und kostet, um es drastisch auszudrücken: Menschenleben. Selbstverständlich dürfen digitale Anwendungen keine Einfallstore für Datendiebstahl bieten, was technisch kein Problem darstellt. Selbstverständlich müssen die im Vergleich zum nicht-europäischen Ausland hohen Datenschutzstandards eingehalten werden, was technisch ebenfalls kein unlösbares Problem darstellt. Dennoch, hier muss noch nachjustiert werden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, weist zu Recht auf die mangelnde Feingranularität hin. Es ist schwer vermittelbar, wieso ein Patient den Befund seiner Psychologin auch seinem Zahnarzt zur Verfügung stellen soll. Mit dem Hinweis, dass die ePA ja freiwillig genutzt werden kann, macht es sich Bundesgesundheitsminister Spahn zu einfach.

Potentiale bleiben ungenutzt

Digitale Daten sind nicht Fluch, sondern Segen

Aber wir müssen auch einen Mentalitätswandel vollziehen. Nach wie vor herrscht in Deutschland ein weitverbreiteter Skeptizismus bezüglich jeglichen technologischen Fortschritts vor. Das betrifft in besonderem Maße auch die elektronische Patientenakte. Bundesgesundheitsminister Spahn legt großen Wert auf Freiwilligkeit, und das ist auch gut so. Wenn es aber nicht gelingt, den breiten Bevölkerungsschichten die Vorteile - und die sind enorm - zu vermitteln, bedeutet Freiwilligkeit auch gleich Irrelevanz. Das kann man sehr gut an der Akzeptanz des Organspendeausweises beobachten. Mit einer elektronischen Patientenakte schaffen wir einen echten Mehrwert für jeden einzelnen Patienten. Dieser muss das aber auch nachvollziehen und wertschätzen. Während Patienten in Dänemark die Sorge umtreibt, ob der gerade behandelnde Arzt auch auf sämtliche relevanten Daten zugreifen kann, um einen möglichst umfassenden Befund abzuliefern, plagt Patienten hierzulande oft die Sorge nach dem Datendiebstahl.

Dass diese Skepsis mit praktischen Lösungen und einer breiten öffentlichen Auseinandersetzung aufgelöst werden kann, zeigt die Corona-Warn-App. Ja, auch hier haben wir im Vergleich zu anderen ein wenig länger gebraucht. Dennoch: Die knapp 20 Millionen Downloads zeigen, die Menschen stehen digitalen Lösungen nicht grundsätzlich ablehnend gegenüber – im Gegenteil. Wir nutzen völlig zu Recht in vielen Lebensbereichen digitale Unterstützung. Unser Alltag ist mit Messengerdiensten, Sprachassistenten, vernetzten Fahrzeugen und vielem mehr längst in einem hohen Maße digitalisiert. Um so wichtiger ist deshalb die Digitalisierung im Gesundheitswesen. Die ePA nimmt hier eine ganz wichtige Rolle ein. Der Zugriff auf oftmals überlebenswichtige Daten ist entscheidend. Der Spruch „Daten teilen – besser heilen“ passte noch nie so gut wie hier und jetzt. //

Daten teilen – besser heilen

PROF. DR. THOMAS JÄSCHKE

vereint seit über 30 Jahren Digitalisierung und Datenschutz. Der Medizininformatiker ist Vorstand der DATATREE AG und unterstützt namhafte Kunden als Datenschutz- und Informationssicherheitsbeauftragter.

Das Patientendaten-Schutz-Gesetz steht vor der Tür

Seit dem 1. Januar 2021 gilt das Patientendaten-Schutz-Gesetz. Der Weg für ein digitales Gesundheitswesen ist damit frei.

Text: Jörg Fecke

Einer der wichtigsten Aspekte ist dabei sicherlich die elektronische Gesundheitsakte. Diese sollte ursprünglich schon vor 16 Jahren, 2004 eingeführt werden. Auch das 2019 verabschiedete Digitale-Versorgungs-Gesetz sah die elektronische Patientenakte vor, doch die Bedenken in Bezug auf den Datenschutz ließen sich nicht einfach wegdiskutieren. Streitpunkt damals wie heute: Die Feingranularität der Akteneinsicht. Nach wie vor ist das Problem nicht vom Tisch. Erst ab dem Jahr 2022 darf der Patient entscheiden, welche Daten er welchem Arzt zur Verfügung stellt. In den ersten zwölf Monaten gilt das Prinzip „alles oder nichts“; dem Bundesdatenschutzbeauftragten Kelber gefällt das nicht.

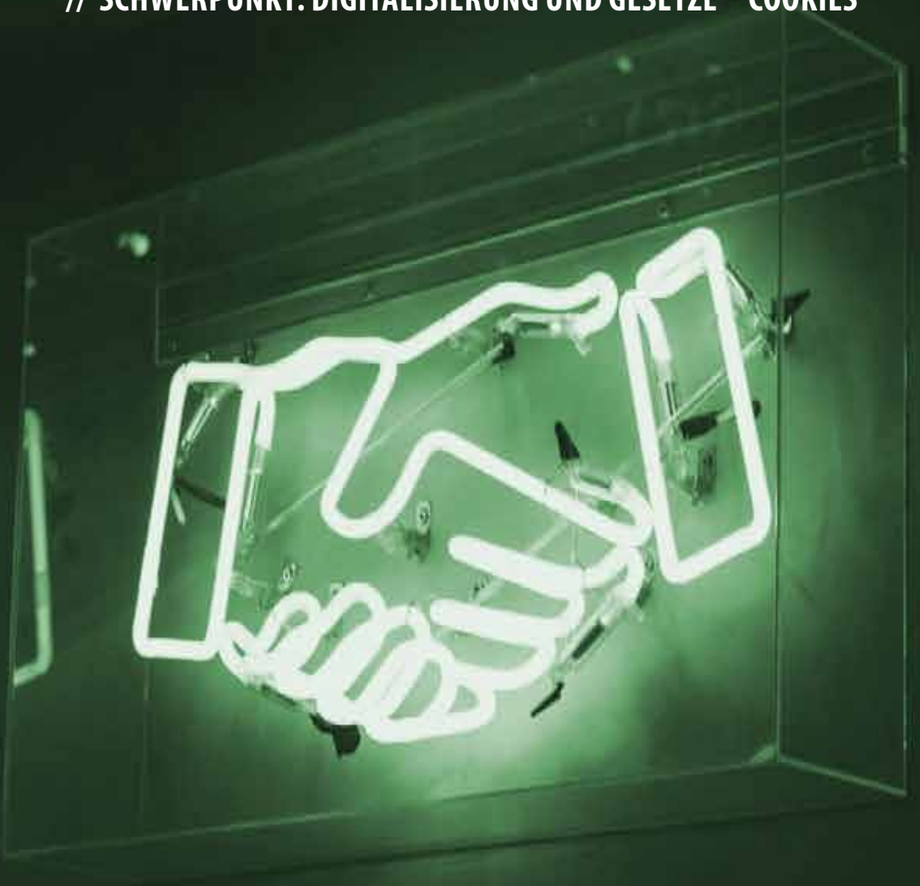
Elektronische Patientenakte erst durch PDSG möglich

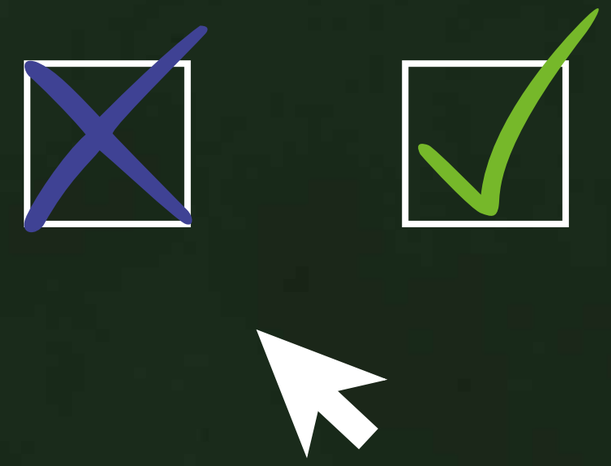
Dennoch: Die Digitalisierung muss gerade im Gesundheitswesen endlich signifikante Fortschritte machen. Die Belastungen werden in Zukunft sicher nicht geringer. Digitale Anwendungen bieten ein enormes Potential der Effizienzsteigerung. Dass hierzulande nach wie vor Patientendaten am liebsten gefaxt werden, erzeugt bei unseren ausländischen Partnern ungläubige Blicke. Dass Ärzte oftmals mehrere Telefonate führen müssen, um alle notwendigen Patientendaten zu erhalten, ist heute auch keine Seltenheit. Das kostet Zeit - Zeit, die wir nicht haben.

Potentiale endlich nutzen

Die elektronische Patientenakte ist dabei nur ein Aspekt. Überweisungen zum Facharzt sollen bald ebenso digital funktionieren wie auch elektronische Rezepte oder elektronische Medikationspläne. Apotheken, Krankenhäuser, Fach- und Hausärzte kommunizieren dann über die Telematikinfrastruktur.

Mit dem Patientendaten-Schutz-Gesetz liefert die Politik den Rahmen, eine Grundlage für das Gesundheitswesen. Dem Datenschutz kommt dabei eine zentrale Rolle zu. Dass die DSGVO berücksichtigt wird, ist eigentlich nicht der Rede wert. Das Gesetz regelt, dass Datenschutz auf höchstem Niveau umgesetzt werden soll, zum Beispiel durch die Datenspeicherung auf ausschließlich deutschen Servern.
Am Ende bestimmen nach wie vor die Patienten, was mit ihren Daten geschieht. Die Nutzung der elektronischen Patientenakte ist und bleibt freiwillig.





Die Einwilligung auf der ersten Seite – nervig oder nützlich?

Jeder kennt sie inzwischen. Bei dem Besuch einer neuen Homepage ploppen sie in allen Formen und Farben auf: Kästen, in denen ein Consent-Management abfragt, welche Daten verarbeitet werden dürfen. Doch was im ersten Moment von fast allen Nutzern als nervig empfunden wird und möglichst mit einem schnellen Klick auf das bereits grün markierte Feld unter der Beschriftung „alles zulassen" erledigt werden kann, sollte man sich noch einmal genauer anschauen.

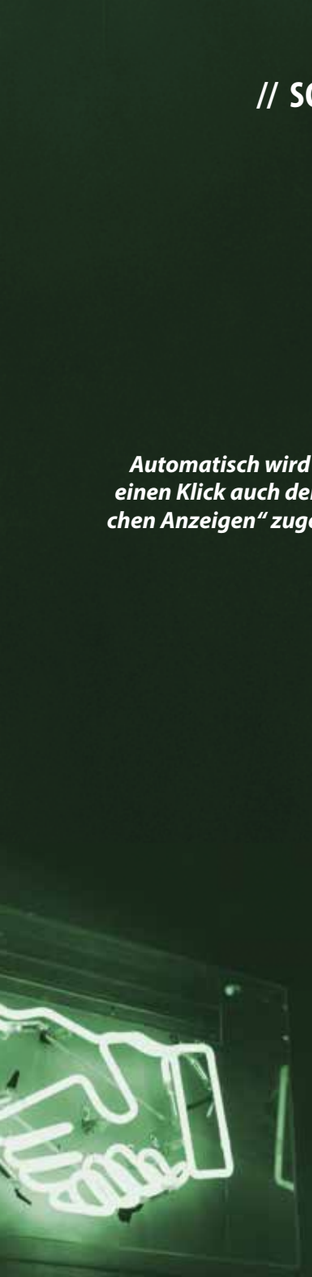
Text: Hanjo Tewes

Was akzeptiert man eigentlich alles und was passiert mit den Daten, wenn man zustimmt?

Ein Blick in die Zwecke der Datenverarbeitung lässt bereits tief blicken, wie die nachfolgenden Auszüge aus der Beschreibung des Consent-Managements einer großen deutschen Tageszeitung zeigen.

Der erste Punkt sind die sogenannten personalisierten Inhalte. Das klingt zunächst unspektakulär, bedeutet aber, dass aufgrund des bisherigen Online-Verhaltens ein Nutzerprofil erstellt worden ist, sodass dem Nutzer individuelle Werbung zugesendet werden kann. Auch das klingt noch harmlos, setzt sich aber z.B. aus meinen historischen Nutzungsdaten im Internet, einschließlich der vorangegangenen Aktivitäten im Internet, und der dadurch offenbarten Interessen durch die Besuche von Homepages zusammen.

Wer der Meinung ist, dass es irrelevant ist, ob eine Tageszeitung diese Inhalte bekommt, sollte sich nicht zu sicher fühlen. Mit dem einen Klick hat man bereits 35 Firmen erlaubt, dass sie dem Nutzer personalisierte Inhalte zur Verfügung stellen. Oder anders formuliert, 35 Firmen können bereits ein Nutzerprofil anhand der oben genannten Faktoren erstellen anlegen und maßgeschneiderte Werbung erstellen.



Automatisch wird mit dem einen Klick auch den „einfachen Anzeigen" zugestimmt:

Für die Auswahl einfacher Anzeigen können Anbieter, so kann man lesen, Echtzeit-Informationen über den Kontext, in dem die Anzeige dargestellt wird, verwenden. Übersetzt bedeutet das, wer nach Autos sucht, bekommt unmittelbar Autowerbung.
Praktischerweise erfragt der Betreiber durch die zuvor erteilte Zustimmung des Nutzers direkt das verwendete Gerät, die Browser-Kennung sowie die IP-Adresse. Die Standortdaten fehlen in diesem Kontext natürlich auch nicht.
Dieser Zugriff auf die oben genannten Informationen inklusive meiner IP-Adresse, welche mich eindeutig identifizierbar macht, wird praktischerweise direkt 93 Anbietern erlaubt.

Weiterhin wurde 104 Firmen mit dem einen Klick (alles erlauben) unter anderem erlaubt, zu messen, wie die Nutzer auf die angezeigte Werbeanzeige reagieren bzw. mit den eingeblendeten Werbeinhalte interagieren.
Es können in diesem Fall bis zu 104 Firmen feststellen, wie Nutzerinnen oder Nutzer auf für sie eingeblendete Werbeinhalte reagieren. Dieses Prinzip ist natürlich für jede Art von Werbung möglich. Das bedeutet, die Messung der Reaktion bzw. Interaktion auf Werbeinhalte funktioniert von Schuhen bis zur politischen Wahlkampfwerbung. Dass dabei so Faktoren wie Verweildauer oder Cursorbewegungen eine zentrale Rolle spielen, ist den meisten Nutzern gar nicht bewusst.

Sofern man nun mit den Gedanken spielt, für unterschiedliche Tätigkeiten andere Geräte zu nehmen, damit nicht zu viele Daten in einem Kontext verknüpft werden - schön gedacht. Die Erlaubnis für die Werbepartner der Homepage zu ermitteln, dass zwei bzw. noch mehr Geräte dem gleichen Nutzer bzw. Haushalt zugeordnet sind, wurde ebenfalls erteilt.

Fazit: Der kurze Blick in das Consent-Management lässt bereits erahnen, wer an den Daten partizipiert und zeigt auf, wie das Online-Angebot einer normalen Tageszeitung zum Daten-Superspreader wird. Wer glaubt, die Zeitung sei ein negativer Ausnahmefall, sollte sich auf eine Enttäuschung einstellen. Wenn man sich die Mühe macht und die Inhalte der Einwilligungen von Homepages mal in Ruhe anschaut, wird feststellen, dass der beschriebene Fall kein Einzelfall, sondern eine weit verbreitete Praxis ist.

Das Positive ist, diese bereits seit Jahren bestehende Praxis wird durch die Regelungen zum Datenschutz bei den meisten Anbietern nun transparent gemacht.

Die Ablehnung zur Datenverarbeitung ist meist nur einen zweiten Klick entfernt. Ob man der Datenverarbeitung zustimmt, kann man jetzt immerhin selbst entscheiden. //

Remote Work? Gerne, aber bitte sicher!

In unserem digitalen Zeitalter ist das Home Office zunehmend Ziel von Kriminellen. Das Arbeiten fern des Firmenbüros ist inzwischen in vielen Unternehmen zentraler Bestandteil des Arbeitsalltags. Damit einher geht laut dem Sicherheitsunternehmen Eset eine Steigerung der täglichen Angriffe von 260 Tausend Anfang des Jahres auf 3 Millionen tägliche Attacken Mitte des Jahres 2020. Die gute Nachricht: Viele Schwachstellen lassen sich mit überschaubarem Aufwand beseitigen.

Text: Jörg Fecke

Anfang März musste es schnell gehen, Corona zwang weite Teile der Arbeitswelt ins Home Office. Seitdem gehören in vielen Fällen Privatgeräte zum Unternehmensnetzwerk. Fragwürdig verteilte Zugriffsberechtigungen haben bis zum heutigen Tag ihre Gültigkeit und in schnell aufgesetzten VPN-Zugängen klafft die ein oder andere Sicherheitslücke. Für die Sicherheit des eigenen Netzwerkes essentielle Prüfungen auf Viren sind teilweise bis heute ausgeblieben.

Wer überhastet handelt, muss Fehler einkalkulieren

In einer repräsentativen Umfrage des IT-Sicherheitsexperten Tanium gaben 85% der Befragten an, dass sie ihr Unternehmen gut vorbereitet auf das Home Office sahen. 90 % der über 1000 Befragten gaben allerdings auch an, dass es zu einem Sicherheitsvorfall gekommen sei. 70% der Befragten entdeckten jede Woche ein neues Gerät in ihrem Netzwerk.

Immerhin, die Gefahren sind allgemein bekannt. Investitionen zur Stärkung der eigenen Abwehrkräfte stehen bei vielen auf der Agenda - bei der Frage des Budgets gehen die Vorstellungen aber nach wie vor auseinander. Das etwas getan werden muss, ist allgemeiner Konsens. Dabei gibt es an einigen Stellen relativ simple und nicht allzu kostenintensive Möglichkeiten zur Angriffsabwehr: Eine Zwei-Faktor-Authentifizierung, die laut 71% der Befragten in ihren Unternehmen nicht existiert, würde einen guten Anfang bilden. In vielen Fällen ist der Zugang zum Firmennetzwerk lediglich mit einem Passwort geschützt. Oft sind Schwachstellen so offensichtlich, dass es ein Stück weit an Fahrlässigkeit grenzt. Gerade durch den einfachen Passwortschutz entwickelt sich das Remote Desktop Protokoll zur Schwachstelle. Das proprietäre Microsoft-Protokoll ist deshalb beliebtes Ziel von Cyberkriminellen.

Gefahr ist allgemein bekannt

Privatgeräte haben in vielen Fällen nicht annähernd das Sicherheitslevel des Firmennetzwerkes. IT-Abteilungen verlieren hier die Kontrolle und wissen oftmals nicht, welch unsichere Gesellen sie sich da ins Netz holen. Dabei muss das Gerät gar nicht erst mit einem völlig veralteten Betriebssystem unterwegs sein – Windows 7 läuft immer noch auf mehr als jedem fünftem Desktop-Rechner. Es gibt nach wie vor genügend Mitarbeiter, die keine oder unzureichend Updates installieren.

Private Endgeräte erschweren die Lage

In letzter Zeit mussten viele erzwungenermaßen auch auf neue Anwendungen zurückgreifen. Den Kontakt mit dem Team hat man dank diverser Videokonferenz-Programme gehalten. Einen Beitrag zur IT-Sicherheit hat man damit weniger geleistet. Ungebetene Gäste haben sich in den letzten Monaten so oft eingeschlichen, dass dafür mit „Zoombombing“ sogar ein ganz neuer Begriff entstanden ist. Wobei es sich hier bei Weitem nicht nur um die Anwendung eines einzigen Anbieters handelt, wie vielleicht der Begriff vermuten lässt.

Neue Anwendungen bringen neue Schwierigkeiten

Es ist wie so oft: Die Lage ist komplizierter als gedacht. Auch wenn es keine Garantien für eine absolut sichere Firmenumgebung gibt: . Viel getan ist schon, wenn das Bewusstsein bei den eigenen Angestellten geschärft und dauerhaft präsent bleibt. Offene Kommunikation auf verschiedenen Ebenen deckt Problemfelder auf und ermöglicht Lösungen, die von allen Beteiligten nachvollzogen und im Idealfall auch beherzigt werden. Die Erstellung eines Kataloges an Handlungsempfehlungen sollten in der Schublade jeder Personalabteilung für den Onboarding-Prozess bereit liegen.

Kommunikation ermöglicht Lösungen

Darüber hinaus gelingt auch mit überschaubarem finanziellen Aufwand eine Reihe an technischen Maßnahmen, die das Sicherheitslevel maßgeblich steigern. Wäre jetzt nicht der richtige Zeitpunkt, um die schon längst angedachte Multi-Factor-Authentifizierung zu etablieren?
Außerdem hilft aufräumen ungemein. Dass es in der Vergangenheit chaotisch zuging, ist entschuldbar - ein ‘Weiter so’ allerdings nicht. //

Ransomwareangriffe – Schutz durch Täuschung

Ransomwareangriffe nehmen stark zu. Oft entdeckt man den Angriff, wenn es für Gegenmaßnahmen schon zu spät ist. Neben klassischen Methoden zur Verringerung des Risikos, wie etwa die Sensibilisierung der Mitarbeiter und eine auf Aktualität ausgerichtete Updatepolitik, gibt es noch eine weitere Maßnahme. Schutz bietet in solch einem Fall auch die Täuschung. Man schlägt Cyberkriminelle ein Stückweit mit ihren eigenen Mitteln.

Text: Maximilian Wölk

In den letzten Jahren haben kryptographische Lösegeld-Angriffe (kurz: Crypto-Ransomware) die Cyber-Bedrohungslandschaft dominiert. Sie zielen auf das wertvollste Gut der heutigen Nutzer von Informationstechnologien und Unternehmen ab: Daten. Crypto-Ransomware verschlüsselt diese Daten, damit sie für ihre Besitzer unzugänglich werden. Wenn die Crypto-Ransomware bei dieser Aufgabe starke Kryptographie verwendet, ist es nicht möglich, dass der rechtmäßige Dateibesitzer den Inhalt der Dateien ohne den Entschlüsselungsschlüssel wiederherstellen kann. Die Opfer, sowohl Benutzer als auch Unternehmen, sind dann gezwungen, ein Lösegeld zu zahlen, wenn sie wieder Zugang zu ihren Daten erhalten wollen und kein ausreichendes Backup oder redundante Lösungen vorhanden sind.

Der Schaden nimmt oft existentielle Ausmaße an

Ransomware hinterlässt normalerweise eine Anweisung auf dem Bildschirm. Nachdem die Opfer das Lösegeld bezahlt haben, stellen die Cyberkriminellen die Dateien bzw. Systeme entweder wieder her oder brechen ihre Versprechen und verschwinden, was zu größeren Verlusten führt. Hinzu kommt, dass Ransomware-as-a-Service (RaaS) auch Personen mit geringem Know-how technischem Know-how ermöglicht, Angriffe zu sehr niedrigem Aufwand durchzuführen.

Crypto-Ransomware verschlüsselt Dateien im System des Opfers. Im Allgemeinen durchläuft Crypto-Ransomware zunächst alle Dateien und führt dann Lese-/Schreiboperationen durch, um sie zu verschlüsseln. Hier kann Schutz durch Täuschung helfen, indem Maßnahmen bei der Dateiübertragung getroffen werden. Man erstellt sogenannte Lockvogeldateien und sorgt so dafür, dass die Crypto-Ransomeware diese zuerst findet und bedient.

Sie erzeugen Dateien, die sich durch Struktur und Namen als Leckerbissen präsentieren. Es ist das Honeypot-Prinzip: Sobald sich die temporale Signatur, die Größe oder andere Eigenschaften dieser Lockvogeldateien auf Platten oder Shares ändern, sind sie wahrscheinlich infiziert worden, weil nämlich legitime Applikationen solche Dateien auf keinen Fall nutzen würden. In der Zwischenzeit wird ein Überwachungsmodul implementiert, welches das Verhalten verdächtiger Anwendungen beim Betrieb von Lockvogeldateien beobachtet. Dieser Ansatz kann wirksam sein, denn Lösegeldprogramme verschlüsseln Dateien in der Regel entsprechend der Suchreihenfolge. Wenn nicht, dann würde dieser Ansatz auch funktionieren, da die Durchsuchung von Dateien rekursiv und zuerst in der Tiefe erfolgt. Das heißt, dass Datei-Suchfäden alle Dateien in einem Verzeichnis durchlaufen, bevor sie auf das nächste Verzeichnis zugreifen. Durch diese Methode ist es gleichbedeutend mit dem Platzieren von Täuschungsdateien in jedem Verzeichnis. Daher durchsucht die Crypto-Ransomware beim Durchqueren von Dateien große Mengen von Lockvogeldateien. Es ist erwähnenswert, dass nicht viele Dateien kopiert werden, wodurch eine übermäßige Plattenbelegung vermieden wird.

Die Maßnahme: Schutz durch Täuschung

Die Überwachung dieser Lockvogeldateien lässt sich leicht implementieren, um zu überwachen, ob Änderungen stattgefunden haben. Anwendungen implementieren Dateioperationen durch den Aufruf von zwei Windows-APIs, FindFirstFile und FindNextFile. (Tatsächlich FindFirstFileW und FindNextFileW für Unicode, während FindFirstFileA und FindNextFileA für ANSI). Mit FindFirstFile wird ein Verzeichnis nach einer Datei oder einem Unterverzeichnis mit einem Namen durchsucht, der mit einem bestimmten Namen oder Teil eines Namens mit Platzhaltern übereinstimmt. FindNextFile wird nach FindFirstFile aufgerufen, um eine Dateisuche fortsetzen. Daher konzentrieren wir uns auf jeden der Prozesse, die FindFirstFile oder FindNextFile aufruft. Der Weg zur Beurteilung, ob ein Prozess die beiden APIs aufgerufen hat, ist Hook. Hook ist ein Art der Technik, die zur Veränderung oder Erweiterung des Verhaltens von Anwendungen durch Abfangen von Funktionsaufrufen, Nachrichten oder Ereignissen, die zwischen Softwarekomponenten übertragen werden, dient.

Einfache Methode mit großer Wirkung

Dieser Ansatz wird zu keinem Verlust führen, da die Prozesse zunächst Täuschungsdateien bedienen müssen und erst dann echte Dateien bedienen dürfen, wenn sie die Erkennung bestanden haben. Köder-basierte Strategien wurden erfolgreich eingesetzt, um den Nachweis eines Eindringens in ein Computersystem zu erbringen. //

MAXIMILIAN WÖLK

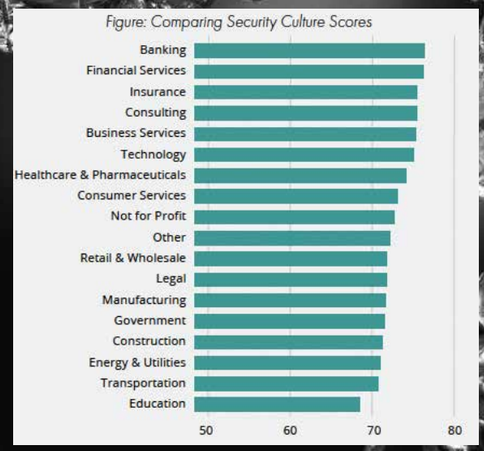
ist Experte für Informationssicherheit bei der DATATREE AG. Zu seinen Kernaufgaben zählt die Prüfung verschiedenster IT-Systeme. Mit Penetration Tests schlüpft Maximilian Wölk in die Rolle eines potentiellen Hackers und deckt so Schwachstellen in den jeweiligen Systemen auf.

Sicherheitskultur in Unternehmen

Text: Annika Raab

Der vom US-amerikanischen Unternehmen KnowBe4 veröffentlichte Security Culture Report 2020 zieht eine ernüchternde Bilanz. Es gibt keine Branche, die ein sehr gutes Ergebnis in Bezug auf ihre Internetsicherheitskultur abliefert. Besonders erschreckend sind dabei die Leistungen von Energie und Versorgung, Transport und Technologie - zentrale Bereiche der KRITIS-Infrastruktur. In diesen Bereichen ist es besonders wichtig, hohe Sicherheitsstandards zu gewährleisten, da bei Ausfällen oder Einschränkungen gravierende Folgen für die Gesamtgesellschaft zu erwarten sind.

Roer, Kai et al. „Measure to Improve. Security Culture Report 2020." KnowBe4, Inc., 2020.



AUSBLICK –
nächste Ausgabe der Exper*Site*:

Informationssicherheit ganzheitlich gedacht –

Stellenwert der Informationssicherheit bei Digitalisierungsvorhaben

Impressum

ExperSite Ausgabe 03 2020 | **ISSN-Print** 2364-5636 | **ISSN-Internet** 2364-5644 | **Herausgeber:** 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 | **Design:** Julia Kleineberg | **Umsetzung:** Julian Hengst, Julia Kleineberg | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titelbild: unsplash, Filip Kominik; S. 2: o.: unsplash, Marius Masalar; li.o.:unsplash, Dylan Ferreira; li. mi.: pixabay, stux; li. u.: unsplash, Khoa Nguyen; S. 3: Tom Schulte, Oberhausen; S. 4-5: pixabay, stux ; S. 6: unspalsh, francois-genon & leonardo-silva; S. 7 unspalsh, Khoa Nguyen; S. 9: pixabay, Hatice EROL; S. 10: Ludger Dudziak, Contilia GmbH, Essen; Sven Schlegel, Arnstadt; Annika Raab, Mainz; S. 11: unsplash, hao-wang; S. 12: unspalsh, Steven Ramon; S. 13: Nicole Effinger, Butzbach; Hintergrundbild: unsplash, Clyde He; S. 14-15: Hintergrundbild: unsplash, Clyde He S. 16-19: unsplash, Jeremy Bishop; S.20-21: Hintergrundbild: unsplash, Ferenc Horvath S.21: Tom Schulte, Oberhausen; S. 22-23: unsplash, Marius Masalar; Tom Schulte, Oberhausen S. 24-26: unsplash, charles-deluvio; S. 27: unsplash, privecstasy; S. 29: unsplash, Note Thanun; S.30: unsplash, Tobias Tullius; Tom Schulte, Oberhausen; S. 31: unsplash, Jilbert Ebrahimi; S.32:unsplash, Loic Leray