Handelsblatt
RESEARCH INSTITUTE

the health circle

Im richtigen Zusammenspiel mit Sicherheit punkten

secunet

Einleitung

Die Digitalisierung des deutschen Gesundheitswesens schreitet voran. Zwar hat der Prozess hierzulande später begonnen als in anderen Ländern – und geht langsamer voran als dort. Doch die Richtung stimmt. Inzwischen werden immer mehr Gesundheitsdaten nicht mehr auf Papier festgehalten, sondern digital erfasst, transportiert und verarbeitet. Gleichzeitig ist die Menge, Breite und Qualität der Daten im Zuge des technologischen Fortschritts – etwa im Bereich der Medizintechnik – deutlich gestiegen.

Diese Digitalisierung der Daten ist die zentrale Voraussetzung dafür, dass all die Mehrwerte realisiert werden können, die sich das Gesundheitswesen von der Digitalisierung verspricht: Wenn Ärzt:innen und andere Fachkräfte im medizinischen Alltag sofort und überall Zugriff auf die relevanten Daten haben, kann dies die medizinische Versorgung und Vorsorge besser und effizienter machen. Es kann also geschafft werden, was sonst selten möglich ist – nämlich Qualitätsverbesserungen bei gleichzeitigen Kosteneinsparungen. Und wenn Forscher:innen auf Daten in großer Breite und Menge Zugriff haben, so können sie daraus mit Hilfe von Big-Data-Analysen und künstlicher Intelligenz Erkenntnisse ableiten, die früher nicht möglich gewesen wären. Auf diese Weise beschleunigt die Digitalisierung den medizinischen Fortschritt.

Um die Digitalisierung der medizinischen Datenwelt voranzutreiben, sind leistungsstarke und sichere IT-Infrastrukturen notwendig. Da ein Großteil der Mehrwerte nur dann realisiert werden kann, wenn die Daten kollaborativ – also von mehreren Akteur:innen gleichzeitig – genutzt werden, wird über den Einsatz von cloudbasierten Lösungen diskutiert. Diese sollten nach Möglichkeit international kompatibel sein. So plant die Europäische Kommission die Einführung eines europäischen Datenraums für medizinischen Daten bis 2025.

Die Konvergenz der Daten und die zentrale Haltung von hochsensiblen Daten bedarf eines entsprechenden Sicherheitsniveaus. Die Risiken wachsen: Wenn Patient:innendaten von einer ärztlichen Praxis gestohlen werden, ist der Schaden begrenzt. Wenn aber Daten einer zentralen Plattform entwendet werden, ist der Schaden enorm.

Der richtige Schutz der kritischen Daten ist somit der zentrale Dreh- und Angelpunkt für zentralisierte Infrastrukturen. Gerade in Deutschland ist die Skepsis in der Bevölkerung groß, die eigenen Gesundheitsdaten zur Verfügung zu stellen und zentral speichern zu lassen. Auch niedergelassene Ärzt:innen tun sich oft schwer damit, die von ihnen erhobenen Daten mit anderen Akteur:innen des Gesundheitswesens zu teilen. Die Sorge vor einer missbräuchlichen Nutzung der Daten überwiegt in vielen Fällen noch die Hoffnung auf einen Zusatznutzen, der durch die kollaborative Nutzung der Daten entstehen könnte. Nur wenn das Vertrauen der Menschen in die Sicherheit der Daten wächst und sich der Nutzen für jeden manifestiert, kann diese Sorge mittel- bis langfristig einer größeren Offenheit weichen. Doch Vertrauen ist nur solange möglich, wie es zu keinem großen Schadensfall kommt und der Mehrwert sichtbar wird.

Vor dem Hintergrund der skizzierten Spannungsfelder vollzieht sich derzeit der digitale Wandel im Gesundheitswesen. Für Deutschland lässt sich attestieren, dass der Aufbau von digitalen Datenplattformen im Gesundheitswesen zwar begonnen hat, insgesamt aber sehr schleppend verläuft. Dies gilt für medizinische Anwendungen im Allgemeinen genauso wie für Patient:innenplattformen im Speziellen.

Welche Herausforderungen erschweren den Aufbau von leistungsfähigen Datenplattformen im deutschen Gesundheitswesen? Zwar sind meist alle notwendigen Bedingungen für erfolgreiche Projekte vorhan-

den: Hier ist zum einen der Wille zu nennen – also der Wunsch nach einem gemeinsamen Vorhaben. Zum Zweiten das nötige Können – also die technologischen Fähigkeiten und Bestandteile. Und zum Dritten die regulatorische Möglichkeit – also ein Rechtsrahmen, der das geplante Vorhaben erlaubt und regelt.

Trotzdem sind die genannten Bedingungen oftmals noch nicht hinreichend, um erfolgreiche Projekte auch tatsächlich realisieren zu können. Es gilt, dass die jeweiligen Akteur:innen in ihren Fachdomänen das Beste leisten und ideal mit den jeweils anderen Domänen verknüpft werden – und nicht versuchen, die ihnen fachfremden Bereiche mitzuverarbeiten.

Reibungsverluste im Aufbau vielschichtiger Lösungen sollten möglichst vermieden werden. Bei Plattformprojekten sind eine Vielzahl von Ebenen beteiligt – von den Anwender:innen über die Anwendungsentwickler:innen und Infrastrukturbetreiber:innen bis hin zu den Komponentenlieferant:innen. Koordinationsprobleme sind zwar nicht erstaunlich, dennoch können sie die Vorhaben in der Digitalisierung des Gesundheitswesens behindern, teilweise gar zum Erliegen bringen.

Für wegweisende Erfolge bei der Digitalisierung scheinen die Bedingungen noch nicht ausreichend gut gesetzt. Es fehlen koordinative Mechanismen und Logiken. Gleichzeitig scheint die Regulatorik noch zu viele Unklarheiten zu lassen. So wird des Öfteren bemängelt, dass die Datenschutzregularien im Alltag schlecht händelbar sind. Hinzu kommt, dass für viele Prozesse (Zulässigkeitsfragen, Austausch mit zuständigen Behörden etc.) und Verfahren (Sicherheitsvorgaben für digitale Gesundheitsanwendungen) noch keine technischen Standards definiert sind, auf die zurückgegriffen werden kann.

Das vorliegende Playbook skizziert, welche Akteur:innen beim Aufbau von Plattformen im Gesundheitsbereich beteiligt sind, vor welchen Herausforderungen diese im Einzelnen stehen und welche Bedürfnisse diese haben in Bezug auf den Aufbau und die Funktionsweise der Plattformen. Außerdem werden Gründe für die beschriebenen Reibungsverluste bei der Zusammenarbeit genannt und Möglichkeiten aufgezeigt, wie die Zusammenarbeit der Beteiligten in Zukunft belastbarer gestaltet werden kann. Bei den Betrachtungen steht der Bereich der Datensicherheit meist im Vordergrund, beleuchtet werden aber auch weitere Aspekte der kollaborativen Datennutzung.

Die Akteur:innen

Im Folgenden werden nacheinander die Akteur:innen genannt, die für die Entwicklung, den Betrieb und die Anwendung von Plattformen im Gesundheitswesen relevant sind. Der Begriff Plattform kann dabei sehr weit gefasst werden. Im Prinzip sind darunter alle Anwendungen zu fassen, bei denen Nutzer:innen auf organisations- und gruppenübergreifende Lösungen zugreifen können, um Daten zu erheben, zu speichern, zu nutzen oder zu teilen. Vor diesem Hintergrund ist schon eine App, die Blutzuckerwerte überwacht und an die behandelnden Ärzt:innen weiterleitet, als Teil einer Plattform zu verstehen. Auch die Krankenhausinformationssysteme, in denen Kliniken die Daten ihrer Patient:innen sammeln, stellen Plattformen dar. Ebenso hinzuzuzählen sind Register, in denen Leistungserbringer:innen Daten für bestimmte Erkrankungen – wie etwa Krebs – zusammenführen und gemeinsam nutzen.

01

Datenspender:innen

Als erstes zu nennen sind jene, die die Daten bereitstellen, die in den Plattformen gespeichert und verarbeitet werden. Dies sind in den meisten Fällen die Patient:innen. Gespeichert wird alles, was relevant ist für eine erfolgreiche Therapie: Vitalwerte, Untersuchungs- und Behandlungsprotokolle, Medikationen, Therapiefortschritte, Laborwerte oder auch Abrechnungsdaten. Die Wünsche der Patient:innen in Bezug auf die Datenplattformen sind meist schlicht, aber eindeutig: Zunächst einmal wünschen sie sich, dass die digitalen Hilfsmittel für sie überhaupt verfügbar sind. Wenn dies der Fall ist, sollen die Plattformen möglichst ihren Zweck erfüllen, sicher sein und – falls die Patient:innen ihre Daten selbst erheben – leicht, barrierefrei und altersunabhängig zu bedienen sein.

Tatsächlich ist die Bedienbarkeit ein zentraler Punkt: Die Digitalisierung kann nur funktionieren, wenn die Beteiligten mit den Technologien auch umgehen können. Ferner werden die Patient:innen die Nutzung von Plattformen dann befürworten, wenn sie auf die Sicherheit der Daten vertrauen können – und wenn sie sich von der Nutzung einen Mehrwert in Bezug auf ihre Gesundheit erhoffen.

02

Systemnutzer:innen

Neben Patient:innen besteht der Nutzer:innenkreis von medizinischen Anwendungen vor allem aus Fachkräften, die etwa in Praxen und Kliniken oder auch in der forschenden Pharmaindustrie oder bei den Versicherungen arbeiten. Die Anforderungen der Nutzer:innen an die Systeme sind ähnlich zu beschreiben wie die der Patient:innen: Ein nennenswertes Interesse an der Architektur der Plattformen besteht nicht. Vielmehr sollen diese stabil funktionieren, einfach zu bedienen sein, die betrieblichen Zwecken erfüllen und Datenschutz sicherstellen. Außerdem sollen die Systeme optimal in die notwendigen Prozesse eingebunden sein und somit eine echte Unterstützung sein und Mehrwerte bieten.

Die Anforderungen an die Systemnutzer:innen im Bereich der Datensicherheit sind groß. Während es den Patient:innen nicht verboten ist, mit den eigenen Gesundheitsdaten sorglos umzugehen und diese auf einer Social-Media-Plattform zu posten, ist dies all jenen strengstens untersagt, die die Daten anderer ver- oder bearbeiten. Zu den Aufgaben, die die Systemnutzer:innen erfüllen müssen, gehört daher eine strenge Beachtung der Sicherheitsvorkehrungen der jeweiligen Organisation. Dies erfordert einerseits das nötige Wis-

sen über die korrekten Abläufe, andererseits ein vorhandenes Problembewusstsein im Umgang mit kritischen Daten. Im besten Fall verhindert das System durch seinen Aufbau einen Missbrauch automatisch. Dies bedeutet beispielsweise, dass das System Methoden anbietet, die nur die Verarbeitung von Daten erlauben, zu denen eine Einwilligung vorliegt.

Grundsätzlich hängt vieles davon ab, ob die Nutzer:innen zur kollaborativen Nutzung der Daten bereit sind. Gerade unter niedergelassenen Ärzt:innen ist die Erkenntnis noch nicht weit verbreitet, dass eine kollaborative Datennutzung viele Mehrwerte schaffen kann. Da die Ärzt:innen allerdings als eine Art Pförtner:innen über die Informationen ihrer Patient:innen wachen, hängt der Erfolg bei vielen Plattformen davon ab, ob diese zur Mitarbeit motiviert werden können. Möglich ist, dass die Nutzung von Plattformen künftig von den Praxismitarbeiter:innen vorangetrieben und eingefordert wird. Schließlich sind sie es, die durch die digitalen Anwendungen im Alltag entlastet werden.

03

Anwendungsentwickler:innen

Plattformen entstehen, indem Systementwickler:innen Anwendungen entwickeln und diese in bestehende Cloudinfrastrukturen aufsetzen. Als Beispiel kann hier eine Smartphoneapp genannt werden, die die Blutzuckermesswerte von einem kleinen Device (Medizinprodukt) aufnimmt, diese an die zentrale Anwendung (Cloud) übergibt und so den behandelnden Ärzt:innen bereitstellt. Da die Entwickler:innen Anwendungen für den Gesundheitsbereich erstellen, dürfte bei ihnen in den meisten Fällen auch ein gewisses Spezialwissen im medizinischen Bereich vorhanden sein. Das Interesse der Entwickler:innen ist, dass die zur Verfügung stehende Cloudinfrastruktur funktional ist und die elementaren Sicherheitseigenschaften und -funktionen bereits von der Plattform zur Verfügung gestellt werden. Von einem tiefergehenden Interesse an der Architektur der Cloudinfrastruktur oder sogar an eigenen Prüfarbeiten bezüglich der Sicherheitstechniken ist nicht auszugehen.

Gerade im Bereich von Datenschutz und Datensicherheit stehen die Systementwickler:innen vor einigen Herausforderungen. So ist die Erfüllung der Regularien für Datenschutz oder Cybersecurity für viele von ihnen nicht trivial. Dies gilt insbesondere für kleinere Software-Unternehmen, die keine eigenen Expert:innen für dieses Thema einstellen können. Ein Problem dabei ist, dass die für die Regulatorik zuständigen Behörden bisher wenig auf die Anwendbarkeit ihrer Vorgaben im Alltag abzielen.

Die Expert:innen für die technischen Systeme können nicht gleichzeitig auch Expert:innen für Regularien und Sicherheitsanforderungen sein. Sie sollten ihre Aufgabe – nämlich die Entwicklung moderner Anwendungen – optimal erledigen und nicht in Interpretations- und Deutungsproblemen der Regularien hängen bleiben.

Auch ist die Regulatorik nicht auf die einzelnen Akteur:innenebenen zugeschnitten, sondern gilt stets universal. Die Folge ist, dass Entwickler:innen eigentlich den gesamten Rechtsbereich überblicken müssten – und sich nicht auf die für sie relevanten Teilbereiche konzentrieren können. Auf diese Weise entsteht mitunter eine Überforderung, die Sicherheitsprobleme zur Folge haben kann. Dies kann beispielsweise vorkommen, wenn Entwickler:innen ihre Software zunächst mit einer zu simplen Benutzer:innenauthentifikation ausstatten, oder wenn die Anwendung durch Quellcodeschwachstellen einfach zum Absturz gebracht werden kann und dann Logiken ausgetrickst und sensible Daten entwendet werden können.

Eine weitere Herausforderung ist die Interoperabilität der einzelnen Anwendungen auf den Plattformen. Für die kollaborative Datennutzung ist es unerlässlich, dass Daten aus verschiedenen Systemen miteinander verknüpft und ausgetauscht werden können. Dafür bedarf es Standards. Viele Anwendungen sind allerdings Insellösungen, die nicht mit anderen Produkten kompatibel sind. Dies kann passieren, weil den Entwickler:innen das nötige Wissen fehlt – entweder, weil es ein kommerzielles Interesse an nicht kompatiblen Lösungen gibt, oder weil schlichtweg noch kein Konsens darüber herrscht, wie Interoperabilität hergestellt werden kann.

04

Infrastrukturbetreiber:innen

Eine andere Gruppe von Akteur:innen sind die Infrastrukturbetreiber:innen. Diese unterhalten Rechenzentren und bieten Cloudinfrastrukturlösungen an. Ihre Aufgabe bzw. ihr Wunsch ist es, Systeme zu schaffen, die den Anforderungen der Datensicherheit und dem sicheren Betrieb entsprechen. Sie müssen also aus den verschiedenen Komponenten der Sicherheits-, Netzwerk- und Hardwareindustrie ein leistungsstarkes System zusammensetzen, in dem Datenverarbeitung und -speicherung vor Diebstahl und Manipulation geschützt sind. Obwohl Wissen und Können vorhanden sind, sind die Akteur:innen auf praktikable Regularien der zuständigen Behörden und zulässige Techniken der IT-Komponentenlieferant:innen angewiesen.

Zu den Problemen der Infrastrukturbetreiber:innen gehört, dass Forderungen zur in Deutschland verfolgten digitalen Souveränität oder zum Einsatz sicherheitstechnologischer Verpflichtungen nicht ausreichend konkretisiert sind. Damit bestehen viele Investitionshemmnisse, gleichzeitig herrscht große Unsicherheit. Im Ergebnis erhalten auch die Systementwickler:innen – als Kunden der Infrastrukturbetreiber:Innen – nicht die fertigen und zulässigen Basisdienste für ihre Anwendungsentwicklung.

05

Komponentenlieferant:innen

Auch die bereits angesprochenen Lieferant:innen von IT-Komponenten für die Cloudinfrastruktur und die entsprechende Sicherheitstechnik stellen eine relevante Gruppe dar. Diese ist zwangsläufig sehr heterogen, da viele unterschiedliche Software- und Hardwarekomponenten verwendet werden müssen. Netzwerktechnik, sichere Betriebssysteme, Sicherheitsmodule oder Storage-System seien dabei nur beispielhaft erwähnt. In der Sicherheitsindustrie geht es beispielsweise um Verschlüsselungstechnologien für den Transport und die Speicherung von Daten, um die Nutzung digitaler Identitäten, um Angriffserkennungssysteme oder um Datenanonymisierungstechniken. Die entsprechenden Komponentenlieferant:innen bieten Schutz für das System als auch Sicherheitsmechanismen für die Daten. Neben der Lieferung von Hardware und Software sind sie dabei auch konzeptionell tätig – und beraten alle anderen Akteur:innenebenen.

Die Komponentenlieferant:innen im Sicherheitsbereich stehen vor dem Problem, dass sie meist als Hauptverantwortliche für die Sicherheit der gesamten Datenplattform angesehen werden, da sie die entsprechenden Bauteile und Verschlüsselungstechnologien liefern. Doch sie können die Sicherheit nicht für die ganze Wertschöpfungskette gewährleisten, schließlich müssen die Vorgaben hinsichtlich Datenschutz und IT-Sicherheit immer auf allen Ebenen beachtet und gelebt werden. Dass sich alle regelkonform verhalten, können die Komponentenlieferant:innen nicht erzwingen.

Folglich wird ihnen eine Verantwortung für etwas zugesprochen, das nur bedingt in ihrem Einflussbereich liegt. Um die Sicherheit in der gesamten Nutzungskette gewährleisten zu können, sind Abstimmungen und eine kollaborative Zusammenarbeit mit allen anderen Akteur:innenebenen nötig. Tatsächlich aber fehlen entsprechende Gremien und Koordinationsmechanismen bisher. Zu den Wünschen der Lieferant:innenebene gehört somit eine verstärkte Koordinierung der Tätigkeiten, außerdem eine stärkere Sensibilisierung aller Beteiligten für das Thema Plattform- und Datensicherheit. Auch Standardisierungen für cloudbasierte Infrastrukturen und Anwendungen wären hilfreich.

06

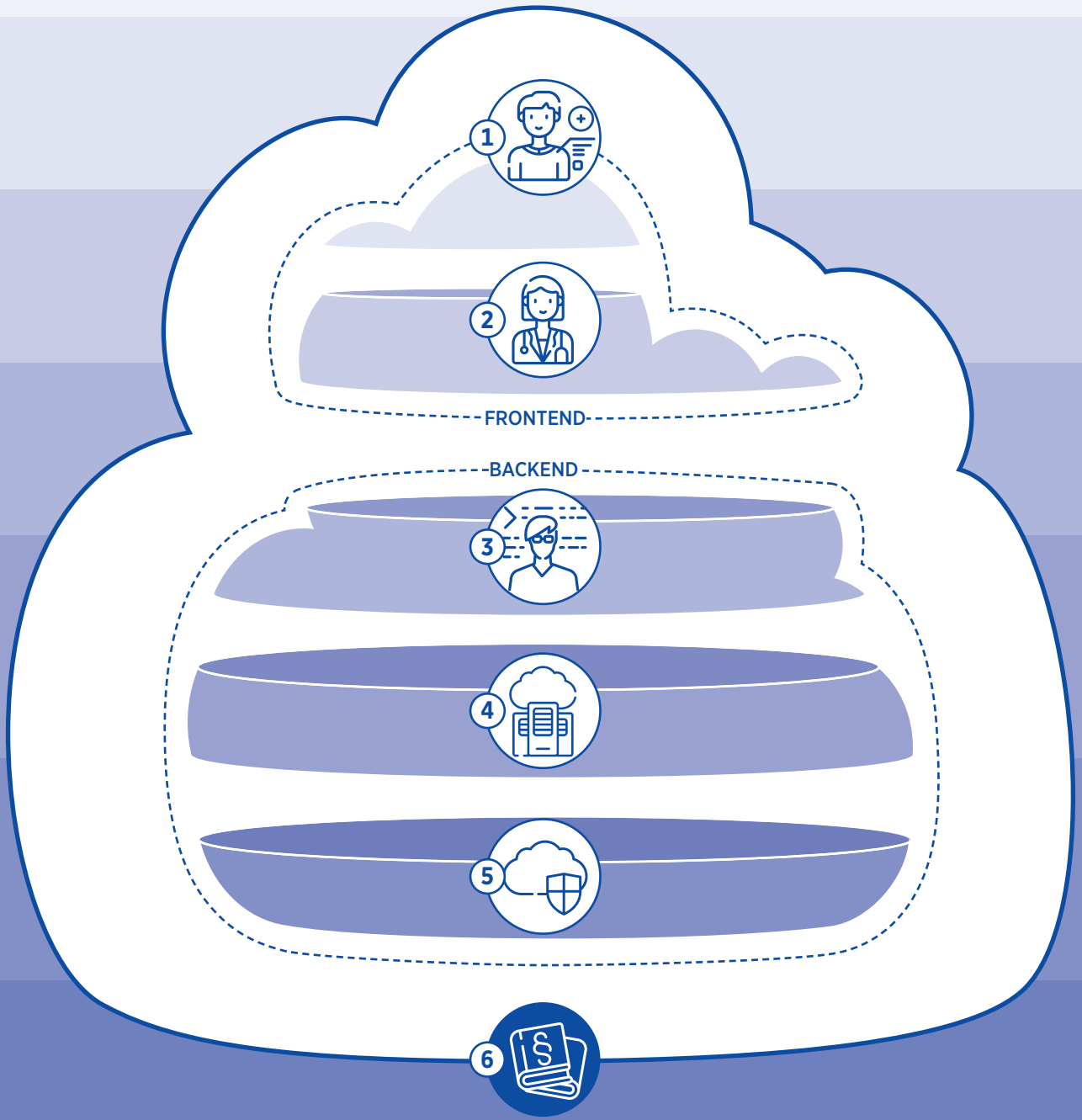
Regulierungsbehörden

Während die bisherigen Akteur:innengruppen als Ebenen in einem aufeinander aufbauenden System betrachtet werden können, steht die letzte zu nennende Gruppe eher neben dem Spielfeld. Gemeint sind die Behörden, die für die Regulatorik und Standardisierungsanreize zuständig sind. Hier sind auf der einen Seite die Institutionen des Gesundheitswesens zu nennen – wie etwa das Bundesgesundheitsministerium (BMG), das zum Geschäftsbereich des Ministeriums gehörende Bundesinstitut für Arzneimittel und Medizinprodukte (Bfarm) oder die Gematik, die für die Telematikinfrastruktur und den deutschlandweiten Gesundheitsdienst zuständig ist. Auf der anderen Seite zählen dazu die mit den Themen Datenschutz und -sicherheit befassten Behörden, wie etwa

das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Datenschutzbehörden von Bund und Ländern. Auch die für die Überwachung und Prüfung von medizinischen Produkten und Verfahren zuständigen benannten Stellen können hier angeführt werden, auch wenn diese keine Regeln vorgeben oder exekutieren – und auch nicht staatlich sind, sondern lediglich staatlich autorisiert.

Als Hüter:innen der grundlegenden Rechtsnormen im Bereich Datenschutz und -sicherheit gehört es zu den ureigenen Interessen dieser Institutionen, die Schutzlevel so zu definieren, dass die entsprechende Regulatorik die gewünschten Ziele erreicht. Kritisiert wird jedoch des Öfteren, dass die Behörden nicht auch das Ziel verfolgen, dass die Regulatorik obendrein gut händel- und anwendbar, also alltagstauglich ist. Beispielsweise ist der Rechtsrahmen im Bereich Datenschutz- und -sicherheit nicht nach Anwendungsbereichen unterteilt, sondern stets in Gänze gültig und anzuwenden. Für die einzelnen Akteur:innen bedeutet dies, dass sie alle Normen im Blick haben müssen, obwohl nur Teilbereiche für sie gelten – was im Alltag eine hohe administrative Hürde sein kann, weil es den Fokus der einzelnen Akteur:innen unnötig von Ihrem Schaffen ablenkt. Sinnvoller wäre hier eine Zusammenarbeit auf Augenhöhe zwischen dem Staat und der Industrie. Im Umgang mit Normierungen und Vorgaben sollte es gut strukturierte Abstimmungen mit den Unternehmen geben, um passgenaue statt pauschale Vorgaben zu machen.

Der deutschen Datenschutzpolitik wird oft attestiert, eine Regulatorik geschaffen zu haben, die den beteiligten Akteur:innen großen Aufwand bereitet, ohne dass dadurch höhere Schutzstandards erreicht werden. Zu nennen sind hier beispielsweise die oftmals je nach Bundesland unterschiedlichen Rechtsrahmen und Verfahren. Diese haben mitunter zur Folge, dass deutschlandweite Projekte nicht realisiert werden können, weil Projektansätze im Bereich Datenschutz nicht miteinander kompatibel sind. Kritiker:innen verweisen oft auf andere EU-Staaten, in denen die europaweite Datenschutzgrundverordnung genauso als Grundlage für die nationalen Regelungen dient wie für Deutschland – in denen aber deutlich alltagstauglichere Detailnormen darauf aufgesetzt wurden.


1
2
FRONTEND
BACKEND
3
4
5
6

1 **PATIENT:INNEN: DIE ANWENDER:INNEN UND SPENDER:INNEN**

Ihre Rolle: Sie profitieren von digital gestützter Versorgung und Gesundheitsanwendungen
Ihre Forderung: Datenschutzkonforme Anwendungen, Vertrauen in Anbieter:innen, Schutz vor Datenmissbrauch
Ihre Aufgabe: Security Awareness, bewusster Umgang mit Angeboten und Datenbereitstellung

2 **ÄRZT:INNEN UND MEDIZINISCHE FACHKRÄFTE: DIE NUTZER:INNEN**

Ihre Rolle: Anwender:innen von medizinischen Anwendungen und Datenverwerter:innen
Ihre Forderung: Moderne und unterstützende Anwendungen, die einfach nutzbar sind und nicht ausfallen
Ihre Aufgabe: Einhaltung von Sicherheitsvorgaben und Sicherheitsmaßnahmen

3 **LÖSUNGSANBIETER:INNEN: DIE ANWENDUNGSENTWICKLER:INNEN**

Ihre Rolle: Anbieter:innen von medizinischen Anwendungen für Kliniken, Labore etc.
Ihre Forderung: Sicherheitsnachweise und –module der Infrastruktur als Basis für eigene fokussierte Sicherheitsmaßnahmen
Ihre Aufgabe: Daten- und Prozessabsicherung auf Anwendungsebene, Training der Nutzer:Innen

4 **HOSTINGANBIETER:INNEN: DIE INFRASTRUKTURBETREIBER:INNEN**

Ihre Rolle: Ordnungsgemäßer und regelkonformer Betrieb der Computer-, Storage- und Netzwerkinfrastruktur
Ihre Forderung: Klarheit in regulatorischen Pflichten und Standards, skalierbare Sicherheitstechnologien
Ihre Aufgabe: Wettbewerbsfähige resiliente Infrastruktur mit hohen Sicherheitsmechanismen bieten

5 **SICHERHEITSINDUSTRIE: DIE KOMPONENTENLIEFERANT:INNEN**

Ihre Rolle: Bereitstellung von Sicherheitsprodukten für digitale souveräne Infrastrukturen und Anwendungen
Ihre Forderung: Sicherheitspolitische Rahmenbedingungen, Standardsetzung für neuralgische Punkte in Gesundheitsanwendungen
Ihre Aufgabe: Zugelassene und zertifizierte Sicherheitsprodukte unter Beachtung von Wirtschaftlichkeit und Usability anbieten

6 **STAAT: DIE REGULIERUNGSBEHÖRDEN**

Ihre Rolle: Sicherheitspolitik und Koordinierung gesamtheitlicher Umsetzungsstrategien
Ihre Forderung: Datenschutz und Betriebssicherheit in kritischen Dienstleistungen des Gesundheitswesens
Ihre Aufgabe: Ordnungsrahmen schaffen und Zielerreichung über sämtliche Akteure koordinieren

Fazit

Wenn leistungsfähige (Patient:innen-)Plattformen aufgebaut werden sollen, ist es notwendig, dass alle beteiligten Akteur:innen eng verzahnt miteinander und im gegenseitigen Verständnis agieren. Allerdings gelingt dies meist nicht optimal. Die Folge sind ein geringes Tempo beim Aufbau der Plattformen und das Risiko von Sicherheitslücken. Es scheint daher dringend angeraten zu sein, die Koordinierung der Beteiligten zu verbessern, ebenso die Verfahren zur Definition von technischen Standards.

Eine enge Zusammenarbeit ist vor allem in Sicherheitsfragen von zentraler Bedeutung. Alle Akteur:innen, die für eine Patient:innenplattform gebraucht werden, sollten sich im Idealfall auf ihre Stärken besinnen können. Dieses bedeutet im Umkehrschluss, dass man die jeweils anderen mit der eigenen Expertise bestmöglich unterstützt. Beim Thema Sicherheit bedeutet dies, dass die Sicherheitssysteme von den Komponentenlieferant:innen so konfiguriert werden sollten, dass die Anwendungsprogrammierer:innen sich nicht darum kümmern müssen, ob in der Plattform alles regelkonform ist. Dementsprechend sollten ihnen zum Beispiel nur jene Schnittstellen angeboten werden, die für das jeweilige Sicherheitsniveau vertretbar sind. Auch die Anwender:innen brauchen Tools, die für sie im Alltag gut nutzbar sind und die ihnen nur jene Zugriffe erlauben, die für den jeweiligen Anwendungsfall relevant sind.

Insgesamt kommt dem Thema Handhabbarkeit eine wichtige Rolle zu. Schließlich lassen sich die Mehrwerte, die man sich von der Nutzung der Plattformen erhofft, nur dann tatsächlich realisieren, wenn die Systeme gerne verwendet werden. Dies gilt für die eigentlichen Nutzer:innen der Systeme genauso wie für jene, die an deren Aufbau beteiligt sind. Obendrein dürften Sicherheitsvorgaben in diesem Fall auch bereitwilliger befolgt werden.

Auf die alltägliche Anwendbarkeit der Verfahren und Prozesse zu achten, sollte auch eine zentrale Aufgabe für die beteiligten Behörden werden. Im Bereich der Sicherheitsarchitektur bedeutet dies, dass Regularien angeboten werden sollten, die – je nach Anwendungsfall – eindeutig festlegen, welche Anforderungen jeweils Gültigkeit haben. Nur so kann die Gesundheitsindustrie Mehrlevelsicherheitsprodukte schaffen, die immer das zum Anwendungsbereich passende Schutzniveau bieten.

Ganz grundsätzlich sollte an künftige koordinative Einheiten bzw. Logiken die Erwartung gerichtet sein, dass diese förderlich wirken in Bezug auf die Innovationstätigkeit. Dazu ist es wichtig, dass die Behörden den Dialog mit der Industrie ausbauen. In Deutschland wird Innovationsfähigkeit verschenkt, da die mannigfaltigen Erfahrungen und Kompetenzen der Industrie nicht immer Berücksichtigung finden. Durch Erfahrung, Kreativität und den nötigen Pragmatismus lassen sich Lösungen schaffen, die den rechtlichen Vorgaben folgen und breite Interoperabilität auf Basis internationaler Standards schaffen. Dazu sollten die Behörden aber künftig nicht so stark in den Markt eingreifen, sondern sich stattdessen auf die Schaffung bestmöglicher Anreize konzentrieren – oder auf die Prüfung, ob eine Lösung den grundsätzlichen Vorgaben entspricht.

Zu beachten ist an dieser Stelle, dass Sicherheitspolitik im Bereich von digitalen Daten immer auch eine geostrategisch-politische Dimension hat. Wenn europäische Plattformen mit Technologien und Komponenten aus Übersee ausgestattet oder sogar Cloudkapazitäten von dort genutzt werden, dann wird immer auch ein Teil der europäischen Souveränität über die jeweiligen Daten aufgegeben. Künftig wird es darauf ankommen, vorhandene Technologien zu nutzen, ohne in den entscheidenden sicherheitsrele-

vanten Punkten Souveränität aufzugeben. Deutschland kann kein neues Google oder AWS erfinden, aber Deutschland kann mit seinen Komponenten- und Anwendungsanbieter:innen die notwendigen Elemente schaffen, die die vorhandenen Technologien für Gesundheitsplattformen nutzbar machen.

Wenn es um den Aufbau von Patient:innenplattformen geht, hat der Staat in Deutschland in den letzten Jahren eine sehr aktive Rolle eingenommen. Statt sich auf das Orchestrieren von Märkten oder das Prüfen von Produkten zu beschränken, agierte man eher in der Rolle von Entwickler:innen und Anbieter:innen. Dass der Staat tatsächlich zentrale Plattformprojekte bis ins Detail selbst plant und umsetzt, erscheint nach den Erfahrungen der zurückliegenden Jahre aber keineswegs sinnvoll. Hier sei vor allem an das Beispiel der Gematik erinnert, also an das System, über das Praxen, Kliniken und Versicherungen digitale Informationen austauschen können. Dieses wurde von staatlicher Seite zentral geplant, was das Projekt sehr schwerfällig und unflexibel gemacht hat.

Immerhin findet auch hier bereits eine Umstellung auf Prozesse statt, bei denen den Auftragnehmer:innen eine größere gestalterische Rolle zukommt. Aber dieser Prozess steht auch erst am Anfang. Ganz generell ist es wichtig, dass Plattformprojekte in Bezug auf den Funktionsumfang und den Nutzer:innenkreis nicht starr gestaltet werden, sondern auch im Nachhinein erweitert bzw. angepasst werden können. Nie darf der Blick auf den eigentlichen Nutzen aus dem Fokus geraten.

Insgesamt erscheint es angebracht, bei der Suche nach geeigneten Koordinierungsmechanismen bzw. -logiken auch die Erfahrungen anderer Branchen in den Blick zu nehmen. Gerade bei der Einigung auf technische Standards blicken beispielsweise Industrie und Handwerk auf eine jahrzehntelange Tradition der Konsensfindung innerhalb der Selbstverwaltung zurück. Wenn die – noch relativ junge – Internetbranche ähnliche Gremien und Strukturen herausbilden möchte, könnte es somit sinnvoll sein, bei diesen Branchen nach Vorbildern zu suchen.

Zusammenfassend lässt sich sagen, dass Patient:innenplattformen zweifelsohne enorme Mehrwerte für das Gesundheitssystem und die Patient:innen bringen kann. Der Lebensstandard in einem Land kann wachsen, die Krankheitslast sinken und der Fortschritt beschleunigt werden. Möglich ist dies allerdings nur, wenn die Plattformen sinnvoll geplant werden und sicher funktionieren. Dies gelingt bisher nur schlecht. Auch deshalb hinkt Deutschland bei der Digitalisierung des Gesundheitswesens im europäischen Vergleich so weit hinterher.

Um leistungsfähige und sichere Plattformen aufzubauen, braucht es dringend ein Mehr an Zusammenarbeit. Die Suche nach geeigneten Koordinierungsmechanismen und -gremien sollte möglichst bald angegangen werden. Gleichzeitig braucht es ein Umdenken auf allen Ebenen: Nur wenn jede beteiligte Ebene eine klare Rolle findet und die eigenen Aufgaben verlässlich erledigt, können Plattformprojekte schneller umgesetzt und zum Erfolg gebracht werden.

Expert:innen-einschätzung von secunet

Weniger Power Play Einzelner, mehr koordinierte und kontinuierliche Offensive von allen Akteur:Innen

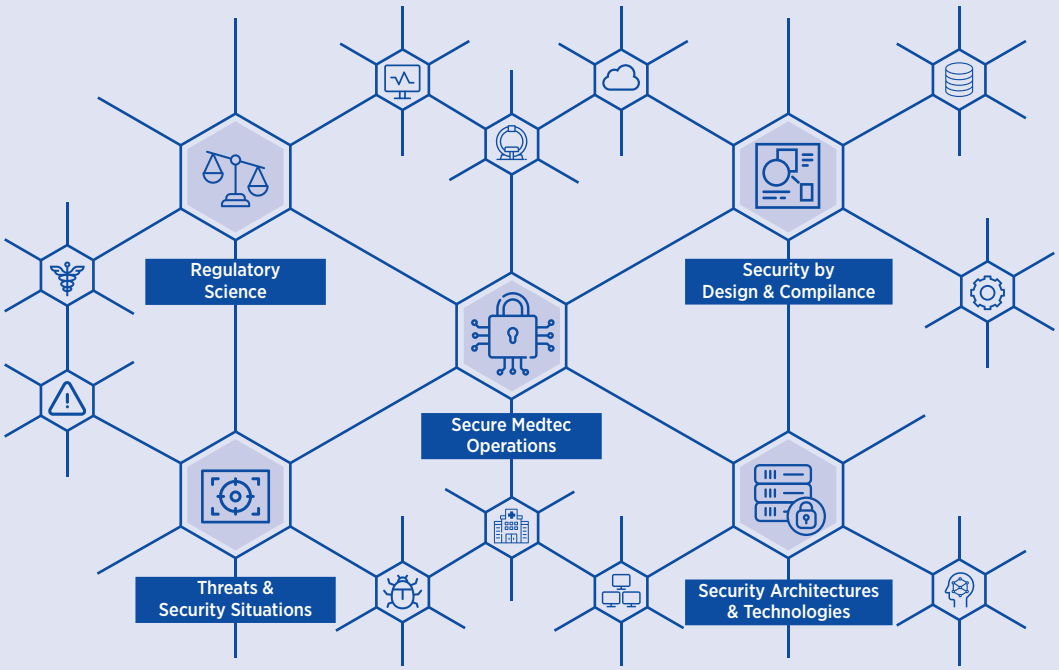
Das langsame Voranschreiten der Digitalisierung im deutschen Gesundheitswesen ist nicht dem fehlenden technologischen Fortschritt geschuldet. Eine verlässliche, sichere und interoperable digitale Infrastruktur kann schon heute problemlos gestellt werden. Das Können und Wollen leidet vielmehr unter der Vielzahl an Marktakteuren und den daraus resultierenden Hürden:

- Wir brauchen Freiwilligkeit als Grundvoraussetzung für den anstehenden Wandel.
- Die gesellschaftliche Akzeptanz für innovative Lösungen ist zwar vorhanden, jedoch gibt es im Gesundheitswesen höchstens gelegentlich eine tatsächliche Konsumentensouveränität.
- Es muss eine Gesetzgebung geschaffen werden, welche einen schnellen und pragmatischen Weg der Umsetzung ebnet.
- Ein gemeinschaftliches Projekt braucht Barrierefreiheit als Wachstumstreiber. Die Silos müssen aufgebrochen, der Dialog forciert werden.

Es ist festzuhalten: Wir könnten schon, sind jedoch noch nicht bereit. Perfektion ist nicht immer der richtige Ansatz für Veränderungen, man darf sich in der Komplexität nicht verlieren. Vielmehr sollte das Streben nach Einfachheit und Effizienz in den Vordergrund gestellt werden. Das Gebot der Simplifizierung unter Berücksichtigung unerlässlicher Regularien zum Wohle der Patient:innen.

Security und Privacy by Design

Häufig beworben, ist es dennoch ein herausforderndes Unterfangen, die relevanten Sicherheitsanforderungen im Blick zu behalten. Wertvolle Compliance-Vorgaben resultieren aus zielgerichteter Regulierung, die sich wiederum an aktuellen Gefährdungslagen und Schadensszenarien der Branche ausrichten. Sicherheitstechnische Konzepte und Betriebssicherheit sind somit stark beeinflusst. Durch eine ständige Überwachung der Sicherheitslage durch branchenweit agierende Organisationen oder Behörden ändern sich diese stetig und werden über passende Prüfvorschriften durch Gesetzgeber oder zuständige Dritte auferlegt.



secunet betrachtet diese Domänen für sich und stellt Zusammenhänge heraus und unterstützt das Zusammenspiel – mit dem Ziel, dass Regulierung praxistauglich gesetzt und später mit Überzeugung umgesetzt wird. Ein wichtiger Aspekt in der Akzeptanz von Sicherheitsvorgaben ist die Anwendbarkeit. Über Forschungsprojekte und die Entwicklung von Werkzeugen zur Umsetzung von Best Practices, Standards und Zulassungsvorgaben versuchen wir Lösungsanbieter und Infrastrukturanbieter in der Produktentwicklung zu unterstützen sowie die richtigen Sicherheitsarchitekturen und Maßnahmen umzusetzen.

Kooperationen für mehr Synergien und Schnelligkeit

secunet Security Networks AG ist als Firma dem Endanwender selten ein Begriff. Wir arbeiten den eigentlichen Lösungsanbietern zu und sind Teil der Lösungen. Unser Ziel ist, dass gesetzliche Pflichten und Sicherheitsvorgaben durch unsere Kunden befolgt werden können. Die enge Zusammenarbeit bereits in der frühen Phase der Produktentwicklung mit Lösungsanbietern ist wichtig. Warum eigentlich? Die Lösungsanbieter können die Vielfalt an Sicherheitsanforderungen und Sicherheitsmaßnahmen nicht eigenständig bewältigten – vor allem dann nicht, wenn neue Sicherheitstechnologien gefordert werden und Sicherheitstechniken kontinuierlich weiterentwickelt werden müssen.

Bringt man in zulassungsrelevante Systemelemente zu wenig Ressourcen und Knowhow ein, mangelt es schnell an Reifegraden für den breiten Erfolg und an der Skalierbarkeit der Lösungen. Fehlendes Knowhow über die Medizinprodukteentwicklung und die Wege zur „Zulassung“ lassen sehr vielversprechende Lösungen häufig auch in Frühphasen scheitern. Hier braucht es fertige, geprüfte und zugelassene Systembausteine, auf die Infrastruktur- und Lösungsanbieter zurückgreifen können, um ihre eigenen Produkte aufzusetzen.

Die Bereitstellung von akzeptierten und nutzerfreundlichen Sicherheitstechniken und -produkten verlangt für sich allein bereits hohe Leistungsstärke, Führungsstärke und Kapazitäten an Expert:innen. Hier treten wir als secunet ein und agieren als Sicherheitspartner mit langjähriger Erfahrung, umfassender Expertise, der nötigen Ausdauer und der Absicht, langanhaltende Beziehungen zu pflegen. So ist es uns möglich, mit verschiedenen Akteueren:Innen im Gesundheitswesen an wegweisenden Gesundheitsplattformen zu arbeiten.

Leuchtturmprojekte in Branchenstandards übersetzen

Es gibt verschiedene Initiativen in der Gesundheitswirtschaft, neue digitale Mehrwertdienste zu erfinden, zu verproben und nachhaltig zu positionieren. Diese reichen von der Telematikinfrastruktur bis hin zu DiGA, DiPA, zu Datenintegrationsplattformen, zu Prozessautomation in Kliniken und neuen Behandlungstechniken. Dabei sind nicht selten isolierte Sichten und individuelle Stoßrichtungen im Gange, die für sich allein genommen nicht im Branchenstandard enden.

Der Einsatz von Cloudinfrastrukturen und die dafür notwendigen Sicherheitsvorgaben sollten unabhängig davon gelten, ob kritische Daten durch das Krankenhaus, den Leistungserbringer, das Labor, den DiGA-Anbieter oder die Versicherung verarbeitet werden, die Absicherung von verarbeitenden und speichernden Systemen in gleichem Maße. Auch die sichere Datenübertragung oder der Zugriff auf Daten für beispielsweise analytische Aufgaben dürften sich aus Sicht der Akteur:innen im Gesundheitswesen kaum unterscheiden.

Die Realität fühlt sich häufig jedoch anders an und man verspürt viele Unsicherheiten und Fragen zu sicherheitstechnischen Umsetzungen. Letztlich suchen die Akteur:innen Sicherheiten, um ihre jeweiligen Arbeiten im eigenen administrativ abgegrenzten Leistungsangebot zu bewältigen. Wie ist der Spagat zwischen technischem Fortschritt und hoch reguliertem Umfeld zu bewältigen? Ist es möglich, die Koordination der vielen Initiativen besser zu bündeln, neue Techniken und Konzepte mit dem Ziel zu verproben, auch direkt Regularien und Sicherheitsvorgaben für neue Wertschöpfung weiterentwickeln zu können? Von Beginn an sind die verschiedenen Akteur:innen in einem Boot zu haben und diese mit ihren jeweiligen Sicherheitsanforderungen zu involvieren. Auch internationale Standards sind präsenter denn je und müssen in diesen nationalen Programmen und Standards beachtet werden.

Wir als secunet sind dabei, wenn es um die Entwicklung von Security Building Blocks für sichere Infrastrukturen und Anwendungen geht. Wir bieten Sicherheitsprodukte, die von Infrastruktur- und Lösungsanbietern einfach in Ihre Basis übernommen werden können und auch Zulassungen und Zertifizierungen standhalten. Wir arbeiten ebenso an Industriestandards mit, um Perspektiven zu schaffen und um im Wettbewerb um die besten sichersten Lösungen im Gesundheitswesen unseren Teil einzubringen.

Torsten Redlich
Leiter Geschäftsentwicklung Division eHealth
torsten.redlich@secunet.com

secunet

secunet Security Networks AG – Schutz für digitale Infrastrukturen
secunet ist Deutschlands führendes Cybersecurityunternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z.B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben. Über 800 Expert:innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im Segment Prime Standard der Frankfurter Wertpapierbörse gelistet und erzielte 2021 einen Umsatz von rund 337 Mio. Euro. secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

Handelsblatt
RESEARCH INSTITUTE

Das **Handelsblatt Research Institute (HRI)** ist ein unabhängiges Forschungsinstitut unter dem Dach der Handelsblatt Media Group. Es erstellt wissenschaftliche Studien im Auftrag von Kunden wie Unternehmen, Finanzinvestoren, Verbänden, Stiftungen und staatlichen Stellen. Dabei verbindet es die wissenschaftliche Kompetenz des 20-köpfigen Teams aus Ökonom:innen, Sozial- und Naturwissenschaftler:innen, Informationswissenschaftler:innen sowie Historiker:innen mit journalistischer Kompetenz in der Aufbereitung der Ergebnisse. Es arbeitet mit einem Netzwerk von Partner:innen und Spezialist:innen zusammen. Daneben bietet das Handelsblatt Research Institute Desk-Research, Wettbewerbsanalysen und Marktforschung an.

Konzept, Analyse und Gestaltung

Handelsblatt Research Institute
Toulouser Allee 27
40211 Düsseldorf
www.handelsblatt-research.com

Text: Dr. Hans Christian Müller
Layout: Christina Wiesen, Kristine Reimann
Bilder: freepik.com, flaticon.com