Die Mühen lohnen sich

Datenschutz ist kein Hemmschuh für eine rasche Digitalisierung, meinen Michaela Grundmeier und Thomas Althammer. Die IT-Fachleute zeigen Ansätze für datenschutzkonforme Lösungen.

Lästig, langweilig, bremsend – Kritiker in Sachen Datenschutz finden gerne Vorwände, warum das Thema besser nicht vertiefend betrachtet werden sollte. Und es stimmt: Datenschutz ist anstrengend, denn oftmals fordern die Datenschutz-Grundverordnung (DSGVO) oder Kirchengesetze zum Datenschutz die Auseinandersetzung mit kritischen Fragen, um Persönlichkeitsrechte und den Schutz personenbezogener Daten angemessen umzusetzen. Das ist gut für jede Einzelne und jeden Einzelnen – und eine wichtige Grundfeste unserer Verfassung.

Datenschutz frühzeitig einbinden

Dem Datenschutz wohnt ein großes Potenzial inne. Datenschutzauflagen fordern, sich frühzeitig und umsichtig mit den Chancen und Risiken von Systemen, Verfahren und Projekten auseinanderzusetzen. Datenschutz frühzeitig einzubinden ist entscheidend. Seine Einbindung ist vergleichbar mit der Einbindung von Mitarbeitervertretung und Betriebsrat. Wenn dies bei Vorhaben zu spät passiert, wird Mitbestimmung häufig als verzögernd und lähmend wahrgenommen. Ganz ähnlich verhält es sich beim Datenschutz. Wird die oder der Datenschutzbeauftragte erst spät in den Prozess involviert, ist es möglicherweise zu spät, um wichtige Grundfragen gemeinsam zu klären.

Ein positives Beispiel für einen gut gelebten Datenschutz, von dem alle profitieren, ist die Corona Warnapp (CWA) der Bundesregierung. Während eine Serie von Sicherheitsproblemen und mangelnder Datenschutz die Warnapp Luca bundesweit in die Kritik gebracht haben, hat die CWA von Anfang an auf ein durchdachtes Datenschutz- und IT-Sicherheitskonzept gesetzt, das aus einer umfangreichen Datenschutz-Folgenabschätzung entstand. Daraus hat sich eine stabile, sichere und akzeptierte Lösung entwickelt, während Luca mehrfach nachgebessert werden musste und heute in Expertenkreisen keinen guten Ruf genießt. Die Schlussfolgerung lautet, dass überhastete Veröffentlichungen und zu wenig Zeit für den Datenschutz personenbezogene Daten aufs Spiel setzen.

In vielen Bereichen hinken wir in Deutschland in Sachen Digitalisierung hinterher. Die Gründe sind vielfältig, doch es ist meist der Datenschutz, der oft als haltlose Schutzbehauptung herhalten muss. Er wird fälschlicherweise oft herangezogen, um Vorhaben zu verhindern, die aus anderweitigen Gründen nicht gewollt sind.

So könnte etwa die Entwicklung des deutschen Gesundheitssystems heute schon viel weiter sein. Beispielsweise wird die Telematik-Infrastruktur seit Jahren entwickelt und optimiert. Die zugrundeliegende Technik ist bewährt und ausgereift. Jahrelang gab es Streit um die Einführung und die Anbindung der verschiedenen Akteure. Mal mauerte die eine Seite, mal floss nicht genug Geld. Auch die Selbstverwaltung der Beteiligten ist nicht immer hilfreich. Der Datenschutz ist in diesen Fällen meist nicht das Problem. Es ging oft eher um Machtfragen. Sinnvolle Anwendungsfälle gibt es genug und es würde der Pflegebranche und dem Sozialwesen viele Arbeitserleichterungen bringen, wenn alle Akteure das gleiche Ziel verfolgten.

Betroffene transparent einbeziehen

Im Gesundheitswesen gibt es durchaus auch gute Beispiele, wo man schon deutlich weiter ist. So setzt heute die ambulante Pflege mobile Geräte für Tourenplanung und Dokumentation ein. Sensorik und maschinelles Lernen unterstützen darin, älteren Menschen ein möglichst langes und selbstbestimmtes Leben in den eigenen vier Wänden zu ermöglichen. Ihr Einsatz lässt sich sicher gestalten, weil Anbieter Betroffene transparent einbinden und es eine Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen gibt.

Die Aufgabe der Zukunft ist es, Sicherheit durch Wissen, Kompetenz und Technologie zu vermitteln. Sie besteht auch darin, uns alle und besonders die Generation der älteren Internetnutzer mitzunehmen und digital fit zu machen. Schon heute sind Smartphones bei über 70-Jährigen keine Seltenheit mehr.

Alexa, der Sprachdienst des Onlinehändlers Amazon, hält Einzug in Senioren-WGs und Fitness-Tracker sind so weit verbreitet, dass sich deren Datenpotenzial auch sehr gut für medizinische oder wissenschaftliche Zwecke nutzen ließe.

Gleichwohl müssen wir die Grenze zur Überwachung vorsichtig ausloten. Hier stehen wir aufgrund unserer Geschichte in Deutschland in einer besonderen Verantwortung. Dabei handelt es sich um eine lösbare Aufgabe. Medizinischen Fortschritt abzulehnen oder blindlings auf neue Technologien zu setzen, ist keine akzeptable Alternative. Zu beachten ist, dass Anwendungen bedienerfreundlich und verständlich sind und Vorgaben des Datenschutzes, wie sogenannte Cookie-Banner, die Menschen nicht nur nerven. Vor allem aber müssen wir an dem Verständnis arbeiten, dass kostenlose Dienste nicht ohne Gegenleistung in Form persönlicher Daten realisierbar sind.

Die Gefahren für IT-Systeme, etwa durch Hacker-Angriffe, steigen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge stetig an. Allein 2020 hat sich die Zahl der Schadprogramme wie Viren, Würmer oder Trojaner pro Tag um etwa 370 000 erhöht. Das BSI hat im selben Jahr sieben Millionen Meldungen zu bestätigten Infektionen mit Schadprogrammen an deutsche Netzbetreiber übermittelt. Die Zahl der abgewehrten Angriffe durch Schadprogramme auf die Bundesnetze hat sich im Vergleich zum Vorjahr mehr als verdoppelt, die Zahl der Spam-Emails sogar fast verdreifacht. Erfolgreiche Angriffe auf Unternehmen mit Erpressersoftware oder Datenabflüssen gehören nahezu zur Tagesordnung. Auch die Sozialwirtschaft und das Gesundheitswesen bleiben davon nicht verschont.

Hier kann Datenschutz helfen. Denn die in den Datenschutzauflagen verankerten Prinzipien Datenvermeidung oder Datensparsamkeit und datenschutzfreundliche Voreinstellungen gehen Hand in Hand mit den Anforderungen aus dem Bereich IT-Sicherheit. Ohne diese technischen Maßnahmen würde die Wirkung von organisatorischen Datenschutzmaßnahmen einfach wirkungslos verpuffen.

Nun stellt sich aber die Frage, wie viel IT-Sicherheit tatsächlich benötigt wird und was genau sich hinter dem Stand der Technik verbirgt, den es zu berücksichtigen gilt? Eine gute Antwort darauf gibt eine Handreichung des Bundesverbandes IT-Sicherheit.

Sicherheit bei Entwicklung beachten

Interessanterweise taucht dort auch die sichere Softwareentwicklung auf, welche mittlerweile jedem Entwicklerteam in Fleisch und Blut übergegangen sein sollte. Hier sind also bereits Vorschläge enthalten, wie die Sicherheit der Anwendungen von vornherein berücksichtigt werden kann, ohne dass im Nachgang ungewollte Überraschungen wie bei der Luca-App auftreten.

Solange es beispielsweise gelebte Praxis ist, Updates auf Systemen erst stark zeitverzögert zu installieren und Backup-Festplatten in Arztpraxen ungeschützt und für jeden zugänglich aufzubewahren, scheint es hier noch ein großes Sensibilisierungspotenzial zu geben.

Daher sind die neuen Vorgaben zur IT-Sicherheit im Gesundheitswesen durch das im letzten Jahr in Kraft getretene Digitale-Versorgung-Gesetz zu begrüßen. So hat beispielsweise die Kassenärztliche Bundesvereinigung für Arztpraxen eine konkrete IT-Sicherheitsrichtlinie für kleine, mittlere und große Arztpraxen entwickelt. Die Einhaltung der Vorgaben aus dem Datenschutz und der IT-Sicherheit können dazu beitragen, dass unsere Gesundheitsdaten soweit wie möglich sicher genutzt werden können.

Kontakt:
michaela.grundmeier@finsoz.de
ta@althammer-kill.de

MEHR INFORMATIONEN:
Handreichung zur IT-Sicherheit:
www.t1p.de/aa58y

Autor:in

Michaela Grundmeier
ist Vorstandsvorsitzende von Finsoz.

Thomas Althammer
von der Unternehmensberatung Althammer & Kill ist Fachgruppenleiter IT-Compliance bei Finsoz.

„Datenschutz fordert, sich frühzeitig mit Chancen und Risiken von Projekten auseinanderzusetzen."