Austausch WISPA (Lothar Seite u. Henning Heck) mit Christoph Saatjohann (Studium „IT-Sicherheit“, aktuell Promotion an der FH Münster, Vorträge u.a. auf den letzten CCC Kongressen) am 28.10.2021. Unten wiedergegeben werden im Wesentlichen die Einschätzungen von Hr. Saatjohann rund um die Telematikinfrastruktur & Co.

1. Zentrale Gesundheitsdatenspeicherung – Risiken vs. Vorteile

Risiken

TI bedeutet zentrale Datenspeicherung. Es gibt vier verschiedene Anbieter, damit 4 verschiedene Rechenzentren, wo z.B. die Daten der elektronischen Patientenakten (ePA) liegen werden. Wenn es gelingt, ein Rechenzentrum und die zusätzlichen Schutzmaßnahmen (bspw. Hardware-Sicherheits-Modul oder selbst löschende Server bei Einbruchsversuchen) zu „hacken“, ist das immer noch eine sehr große, potenzielle Datenmenge. Die zentrale Datenspeicherung bedeutet damit theoretisch immer auch ein größeres Risiko als, z.B., eine dezentrale Datenverarbeitung mit einer Ende-zu-Ende-Verschlüsselung.

Vorteile

2005 war ein wichtiges Argument für die zentrale Datenspeicherung, dass dezentral zu wenig Daten gespeichert werden konnten, z.B. auf den Chips der elektronischen Gesundheitskarte (eGK) oder auf USB-Sticks. Das hat sich inzwischen etwas geändert, auch Chips und USB-Sticks können heute relativ große Datenmengen speichern, während, auf der anderen Seite, auch die Speicherkapazität der ePA der ersten Ausbaustufe noch nicht für MRT-Aufnahmen und dergleichen ausreicht.

Vorteile, die bleiben, sind, erstens, dass Daten durch die zentrale Speicherung seltener verloren gehen, und, zweitens, immer verfügbar sind. Der Versicherte muss nicht erst nach dem USB-Stick suchen, um seinem Arzt Einblick in seine ePA zu geben. Durch die professionell betriebenen Rechenzentren mit entsprechenden Backups bleiben die Daten des einzelnen Versicherten auch vor Unwägbarkeiten wie Hochwasser, Erdbeben, oder Diebstahl verschont. Bei einer dezentralen Datenverarbeitung würden regelmäßige Backups das Risiko des Datenverlusts erheblich reduzieren, aber erfahrungsgemäß werden solche nun einmal von den wenigsten durchgeführt.

Ein weiterer Vorteil ist, dass wir mit der Infrastruktur für die zentrale Datenspeicherung künftig einfacher und sicherer auch größere Datenmengen zu Forschungszwecken sammeln können. Das Auswerten dieser Daten kann für einige Forschungsbereiche hilfreich sein, bietet aber auch immer die Gefahr der missbräuchlichen Nutzung. Daher muss eine solche Funktion immer freiwillig und entsprechend transparent ersichtlich sein, in welchem Maße die Daten anonymisiert oder pseudonymisiert sind.

2. Verschlüsselung

Jede ePA hat zwei Schlüssel, man braucht beide Schlüssel, um die Daten der ePA einsehen zu können. Das kann nur der Versicherte selbst, außer ihm hat kein Akteur in der TI Zugriff auf beide Schlüssel. Ein Schlüssel liegt bei dem ePA Aktenbetreiber, der andere Schlüssel liegt bei einem zentralen Schlüsselprovider (D-Trust). Beide Schlüsselprovider sind technisch und rechtlich strikt getrennt. Als Beispiel, Administrator Felix der Firma Megadaten hat einen Schlüssel aus dem gesicherten Schlüssel-Server gehackt, mit dem er aber nichts anfangen kann, weil der zweite Schlüssel sicher auf dem Schlüssel-Server der Firma D-Trust liegt. Es ist rechtlich untersagt, auf Betreiberseite beide Schlüssel zusammenzuführen; auch rein praktisch wäre das ein sehr hoher Aufwand und daher sehr unwahrscheinlich.

Auch wenn es nie eine 100%-ige Sicherheit gibt, sind die Anwendungen der TI mit ihrer Form der Verschlüsselung als sehr sicher einzustufen. Das ist nicht zu vergleichen mit, zum Beispiel, der eingesetzten Technologie der finnischen Psychotherapie-Praxen-Kette Vastaamo, wo 2020 zehntausende Psychotherapiedaten gestohlen wurden.

3. Sensible Daten wie z.B. Psychotherapiedaten

Es gilt immer die Risikoabwägung. Bei sehr sensiblen Daten stellt sich umso mehr die Frage, ob man das Risiko eingehen möchte, die die zentrale Speicherung mit sich bringt. Auch ist der Nutzen hier fraglicher, da sehr sensible Daten nicht in der Häufigkeit und Regelmäßigkeit entstehen. Für meine Psychotherapie einmal mit dem Konsiliarbericht zu meinem Hausarzt zu müssen ist etwas anderes, als für ein Rezept jedes Quartal wieder loszumüssen, bei meinem Arzt Wartezeiten in Kauf zu nehmen und dort womöglich noch in Kontakt mit Corona-infizierten Patienten zu kommen.

Es wäre möglich und auch gut vorstellbar gewesen, einzelne Funktionen nicht über die TI laufen zu lassen, zum Beispiel die sichere digitale Kommunikation KIM. Dann wäre das auch für Psychotherapeuten nutzbar gewesen, ohne sich an die TI anschließen zu müssen.

4. Verantwortungen

Was die Datensicherheit anbelangt, sind die Verantwortungsbereiche inzwischen geklärt (Datenschutzfolgenabschätzung im Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz). Was den konkreten Service im Alltag anbelangt, gibt es hier aber weiterhin Schwächen und Unklarheiten. Eine bessere Lösung als aktuell wäre es, wenn die gematik nach außen hin die Verantwortung hätte, und intern dann die jeweiligen Stellen zur Verantwortung ziehen würde. Konkret: Wenn der Hausarzt oder der Versicherte bei technischen Störungen und Schwierigkeiten sich immer an die gematik wenden könnte, und die gematik dann intern schaut, wo die Baustelle ist und sich hier die entsprechende Stelle heranzieht. So aber werden die Nutzer mitunter zwischen den verschiedenen Stellen - Rechenzentrum A, PVS-Anbieter X - hin- und hergeschoben.

5. Wird das noch was mit der TI?

Die Funktionen rund um die TI rumpeln gewaltig, egal, ob es sich um KIM, eAU, eRezept oder mitunter auch den Stammdatenabgleich handelt. Das Ganze ist ein komplexes System, mit vielen Akteuren, die jeweils wieder ihre eigenen Interessen haben. Das zusammen zu bekommen ist nicht einfach, aber nicht unmöglich. Das kann nach wie vor gelingen, aber die Herangehensweise sollte geändert werden.

Ein großes Problem sind die zeitlich engen Vorgaben „von oben“. So funktioniert gute Softwareentwicklung nicht. Das macht unnötigen Druck, es müssen Abstriche gemacht werden, sei es in der Benutzerfreundlichkeit (usability), in der Sicherheit (security) – oder in beidem. Besser wäre es, das Ziel zu formulieren, den Entwicklern Zeit zu geben, dann nach einem halben Jahr zu schauen, wie weit man ist, Besserungen vorzunehmen – und die Produkte erst dann zu bringen, wenn sie wirklich funktionieren. Wieso musste zum Beispiel die ePA bereits 2021 angeboten werden, obwohl das feingranulare Zugriffsmanagement noch nicht da ist – ein elementarer Bestandteil für die Datenhoheit des Patienten. Auch die damalig angekündigte Einführung des eRezepts ab dem 1. Juli 2021 ist gescheitert und es ist fraglich, ob die verpflichtende Nutzung zum 1.1.2022 durchgesetzt werden kann.

Ein „Moratorium“, wie jetzt von einigen Akteuren gefordert, ist aber nicht die Lösung. Das hatten wir bereits unter Gesundheitsminister Phillip Rösler. War war dann passiert? Die guten Leute bei

der gematik haben gekündigt und sich Jobs gesucht, wo sie etwas voranbringen können. Da wurde viel Zeit verloren.

Münster, 5.11.2021

Henning Heck
In Abstimmung mit Christoph Saatjohann