

FINGERPRINT, IRISSCAN UND CO. IM KRANKENHAUS

Ganz anders als bei James-Bond

Systeme, die körpereigene Merkmale oder charakteristische Verhaltensweisen nutzen, um Menschen Zugang zu gewähren, einen Prozess in Gang zu setzen oder den Wahrheitsgehalt von Dokumenten zu bescheinigen, assoziieren viele Menschen immer noch eher mit einem zweifelhaften Science-Fiction-Szenario als mit der Option Arbeitsabläufe bequemer zu gestalten. Noch denkt man im Zusammenhang mit Biometrie eher an totale Absicherung statt an Komfortgewinn für die Lösung einer Aufgabe, die ohne Biometrie zwar möglicherweise ebenso sicher aber nicht so angenehm, einfach oder zuverlässig bewältigt werden könnte.

Das vor allem auch, weil biometrische Verfahren menschliche Unzulänglichkeiten wie das Verlieren oder Vergessen von Zugangsberechtigungen oder mangelnde Sorgfalt im Umgang mit diesen sensiblen Instrumentarien (jeder kennt die Haftzettel mit dem Passwort an Computern mit sensiblen Patientendaten) ausschalten.

Ob nun am besten die Struktur eines Fingers, das Muster der Iris, das Gesicht oder die Datensignale einer Unterschrift biometrisch ausgewertet werden sollen, um einen Menschen eindeutig identifizieren, authentifizieren oder einen Sachverhalt verifizieren zu können, lässt sich nur mit Blick auf die Einsatzszenarien und vor allen Dingen auch mit Rücksicht auf die Menschen, in deren Workflow das System integriert werden soll, beantworten. „Kein biometrisches Verfahren eignet sich für alle potenziellen Einsatzgebiete im Krankenhaus gleichermaßen“, betont Jörg-Matthias Lenz von Softpro. Ein jedes habe seine besonderen Stärken und Schwächen. Je nachdem, welche Aufgabe gelöst und in welchem Umfeld agiert werden soll, kommen diese unterschiedlich zum Tragen. Lenz empfiehlt hier als Orientierungshilfe den „Teletrust-Kriterienkatalog für den Einsatz biometrischer

Systeme“. Zu finden ist dieser Überblick über die entsprechenden Systeme und ihre Eigenheiten auf der Homepage von Teletrust (www.teletrust.de), einem interdisziplinären Verein, der sich unter anderem der Vertrauenswürdigkeit elektronischer Prozesse widmet.

Einige Beispiele mögen zeigen, wie viele Überlegungen bei der Auswahl eines biometrischen Systems zu berücksichtigen sind: Die Erkennung des Gesichtsfeldes kann vergleichsweise zeitaufwändig sein. Die Zuverlässigkeit dieser Methode hängt außerdem von stets vergleichbaren Beleuchtungssituationen ab – eine Voraussetzung, die in manchen Kliniken nur schwer zu erfüllen ist. Hersteller von Verfahren zur Iriserkennung verweisen gerne auf die angeblich hohe Sicherheit des Verfahrens. Andererseits geht mit der Wahl dieser Methode ein hoher Aufklärungsbedarf einher. Viele potenzielle Anwender wissen nicht, dass für die Auswertung der Iris gar keine Laserstrahlen eingesetzt werden und fürchten um die Gesundheit ihrer Augen. Ganz so einfach ist dieser Irrtum nicht aus der Welt zu schaffen, denn die Kameras für die Iriserkennung werden nach „Laserklassen“ eingestuft und mit dem entsprechenden Hinweis versehen.

In der Praxis entstehen darüber hinaus noch andere Hürden für den Einsatz biometrischer Systeme, die nicht mit der theoretischen Leistungsfähigkeit des Verfahrens als solchem sondern mit den speziellen Bedingungen am Einsatzort zusammenhängen. Ein klares Hindernis für die Verwendung des Fingers als biometrisches Merkmal ist beispielsweise das Tragen von Schutzhandschuhen. Dazu kommen, ähnlich wie bei der Iriserkennung, eher gefühlte als reale Risiken: In Zusammenhang mit der Erfassung des Fingerbildes werden oft auch hygienische Bedenken geäußert. Unterschriften werden mit papierbasierten Prozessen assoziiert. Biometrische Verfahren, denen eine Unterschrift zu Grunde liegt, sind also am besten dort einzusetzen, wo Verwaltungsabläufe



digitalisiert wurden. All diese Beispiele zeigen, dass neben der Praktikabilität der Systeme je nach Einsatzzweck auch die Akzeptanz, die Motivation und die Bereitschaft biometrische Verfahren zu nutzen, eine entscheidende Rolle spielen, wenn man sich für eines davon entscheiden soll. Unverständlich ist für Thomas Brenner, Sales Director bei byometric Systems, deshalb, dass potenzielle Anwender ihr Augenmerk meist ausschließlich auf die Sicherheit dieser Systeme richten: Halte man sich vor Augen, dass die meisten Krankenhäuser einen Großteil ihrer Prozesse und Räumlichkeiten derzeit überhaupt nicht vor unerlaubten Eingriffen und Übergriffen schützen, dann befremde eine Diskussion über die von den biometrischen Verfahren gebotenen Sicherheitsstandards.

Schließlich, ergänzt Ulrich Kipper von it-werke, müssen Krankenhäuser jetzt nicht plötzlich abgesichert werden wie der Hochsicherheitstrakt eines Gefängnisses. Das Pendeln zwischen gar keiner und totaler Absicherung ist für die Anbieter ein bislang unerklärliches Phänomen. Nicht Sicherheit um jeden Preis sondern die Funktionalität im jeweiligen Einsatzgebiet sollte im Krankenhaus das Auswahlkriterium mit der größten Priorität sein. Sicher genug für das Krankenhaus seien die Systeme letztendlich alle.

Noch hat keines der biometrischen Verfahren jedoch den Krankenhausmarkt in großem Stil für sich erschließen können. Dem Zustand des Experimentierens folgte nicht der erhoffte Boom. Dabei scheint das Thema Biometrie im Krankenhaus bislang untrennbar mit dem speziellen Einsatzgebiet der Säuglingsstation verbunden zu sein. Es gibt kaum ein Pilotprojekt, das sich nicht dem besonderen Schutz der kleinsten Krankenhauspatienten widmet. Kritiker sehen dahinter eine Marketingstrategie. Hier werde Geschäft mit einem starken Gefühl gemacht. Sowohl zwischen dem Systemanbieter und dem Krankenhaus, als auch zwischen Krankenhaus und den werdenden Müttern soll hier der Appell an die Fürsorgepflicht die Kassen klingeln lassen. Branchenkenner sehen die für den Einsatz biometrischer Verfahren prädestinierten Szenarien im Krankenhaus an ganz anderer Stelle.

Eine vorrangige Aufgabe für die Krankenhäuser werde es in den nächsten Jahren sein, ihre zunehmend vernetzte IT-Landschaft vor unerlaubtem Zugriff zu schützen. Das gute alte Passwort habe hier ausgedient. Zahllose Anwender werden es begrüßen, dass sie beispielsweise nur noch ihren Daumen über ein Feld auf dem Laptop ziehen müssen, um sich zu authentifizieren.

Eine weitere Entwicklung, der sich das gesamte Gesundheitswesen nicht entziehen kann, ist die zunehmende Digitalisierung der Patientenverwaltung, angefangen bei der Aufnahme des Patienten über dessen Aufklärung bis hin zur Dokumentation der durchgeführten Maßnahmen. Eine Reihe von Kliniken versucht mittlerweile bei all diesen Schritten möglichst viel Papier einzusparen. Biometrische Verfahren sind hierbei kein Selbstzweck sondern

integraler Baustein eines komplexen Gesamtprozesses, der nicht nur juristisch abgesichert werden muss.

Thomas Kleemann, IT-Leiter am Klinikum Ingolstadt, beschäftigt sich bereits seit langem mit diesem Thema und summiert seine Erfahrungen: „Ärzte akzeptieren die digitalen Verfahren nur, wenn sie sich im Vergleich zum Umgang mit Papier möglichst wenig umgewöhnen müssen.“ In Ingolstadt brachte man es im Rahmen eines Pilotprojektes zur digitalisierten Dokumentation daher auf eine einfache Formel: Möglichst leichte Tablett-PCs in Form einer elektronischen Schiefertafel, intelligente Formulare und die eigenhändige Unterschrift als elektronische Signatur. Es sei in unserer Kultur einfach üblich, Dokumente zu unterschreiben. Seinen Praxistest am Klinikum Ingolstadt realisierte Kleemann daher in intensivem Austausch mit dem Unterschriftenspezialisten Softpro.

Das Pilotprojekt in Ingolstadt zeigte, dass und vor allen Dingen wie digitalisierte Verwaltungsabläufe funktionieren können. Der Weg zu einer serienreifen durchgängig erfolgreich digitalisierten Verwaltung braucht nun jedoch das Zutun weiterer Mitspieler. Hier gibt es sowohl bei den Herstellern der Dokumenten-Verarbeitungsprogramme als auch auf Seiten der Hardware-Hersteller noch Nachholbedarf. Zahlreiche IT-Chefs in Kliniken fordern die Hersteller auf, sich hier intensiver mit den Wünschen und Anforderungen in den Kliniken auseinander zu setzen, statt primär zu versuchen, bereits vorgefertigte Lösungen zu verkaufen. Erst dann könne der Absatzmarkt Krankenhaus sowohl von den Biometrie-Herstellern wie auch von korrespondierenden Anbietern wirklich zum gegenseitigen Nutzen erschlossen werden.

Die Erfahrung in Ingolstadt und in anderen innovativen Kliniken zeigt: Der Austausch zwischen den Entwicklern in den Softwarefirmen und den IT-Abteilungen in den Kliniken muss oft erst aufgebaut, oder zumindest fast überall intensiviert werden. Die Anforderungen im Gesundheitswesen sind längst nicht jedem Entwickler biometrischer Software bekannt. Damit die Kliniken wirklich praxistaugliche Systeme erhalten, führt auch für sie kein Weg daran vorbei, den intensiven Kontakt zu den Herstellern zu suchen – bis hin zu gemeinsamen Entwicklungen.

Nicht nur Kleemann sieht es kritisch, Erfahrungen aus Pilotprojekten in anderen Krankenhäusern abzuleiten, ohne diese genauer zu hinterfragen. So soll es schon mal vorkommen, dass Kliniken in der 100-Betten-Klasse eine neue Technologie unter der Prämisse als Pilothaus besonders günstig erwerben, dass sie diese Technik nicht kritisieren. Eine weitere „Fallstudien-Falle“ liege im Betrachten von Beispielen aus dem Ausland, insbesondere den USA. Die Abläufe in den Kliniken im Ausland seien häufig überhaupt nicht vergleichbar mit denen in einem deutschen Krankenhaus. Sehr skeptisch stehen erfahrene IT-Leiter außerdem den oft utopischen Versprechungen der Hersteller in Bezug auf die Wertschöpfung durch ihre Systeme gegenüber. Konkrete eher vorsichtige Berechnungen für das eigene Haus würden sie dieser theoretischen Zahlenakrobatik ganz klar vorziehen. Ebenso wenig hilfreich seien angebliche Analogien zur Authentifizierung bei der Personenkontrolle an der Grenze. Ein Klinikum sei nun mal keine Grenzstation.

Hier gibt es vor dem erfolgreichen Einstieg in den Krankenhausmarkt für so manchen Hersteller biometrischer Systeme wohl noch Hausaufgaben zu erledigen, die deutlich über die Abwicklung des einen oder anderen Pilotprojektes hinausgehen. Der Boden wäre fruchtbar, denn den Krankenhäusern bleibt nicht viel Zeit, um ihre IT-Strukturen sowohl funktionell als auch sicherheitstechnisch auf Vordermann zu bringen. Nun muss nur noch das Saatgut für den Boden optimiert werden.

Im Bereich der Zutrittskontrolle haben die biometrischen Verfahren übrigens einen starken Mitbewerber. Je nach Einsatzgebiet passt der Chip auf der Plastikkarte zuweilen besser ins Konzept. Mittelfristig gehe hier der Trend – so die Hersteller – zur kombinierten Lösung. Biometrische Merkmale lassen sich auch auf dem Chip speichern. Schon heute sollten sich Kliniken jedoch in jedem Fall mit der Frage auseinandersetzen, wo biometrische Merkmale die Arbeitsabläufe sinnvoll abrunden können. Nur wer seinen Wunschzettel geschrieben hat, wird auf dem Markt das jeweils passende System finden oder in Auftrag geben können. ■

Maria Thalmayr