Auch ein Smartphone kann als zweiter Faktor für mehr Sicherheit bei der Authentifizierung dienen. Schwierig wird es allerdings dann, wenn das Gerät einmal nicht zur Hand ist.

Schutz von Patientendaten

Zwei Faktoren für mehr Sicherheit

Wenn sensible Gesundheitsdaten über das Internet ausgetauscht werden, steht die Absicherung von Zugängen und Übertragungen an erster Stelle. Sicherheitsexperten empfehlen zum Schutz der Daten die Zwei-Faktor-Authentifizierung.

Die Digitalisierung des Gesundheitswesens wird begleitet von der Sorge, sensible Daten könnten in falsche Hände geraten. Beispiele für die Anfälligkeit von IT-Systemen für Cyberangriffe gab es jüngst viele.

Datenschutzexperten wie Christoph Rösseler, Sprecher des Sicherheitssoftware anbieters G-Data, weisen darauf hin, dass klassische Passwörter und PINs keinen ausreichenden Datenschutz bieten: „Um Onlinezugänge zuverlässig zu schützen, sollte dringend eine Zwei-Faktor-Authentifizierung eingesetzt werden."

Zwei Faktoren für mehr Sicherheit

Bei diesem Konzept werden statt nur einem Sicherheitsfaktor, wie einem Passwort, zwei Faktoren gefordert. Das Prinzip ist schon lange im Einsatz – etwa beim Online-Banking, wo für Überweisungen neben der persönlichen Identifikationsnummer (PIN) auch eine Transaktionsnummer (TAN) erforderlich ist, die etwa von einem Codegenerator – einem Token – erzeugt wird. „Wichtig ist, dass die beiden Faktoren unterschiedliche Eigenschaften haben, wie die Kombination aus Wissen und Haben: Der Nutzer weiß seine Zugangsdaten, und er hat ein Token", so Rösseler.

In leicht abgewandelter Form kann als zweiter Faktor auch ein Smartphone dienen, auf dem eine App den PC-Login über einen unabhängigen Kanal bestätigt. Die Zwei-Faktor-Authentifizierung fordert das Bundesgesundheitsministerium explizit bei den Anforderungen an eine virtuelle elektronische Gesundheitskarte.

Kassen koppeln Accounts

Auch die von mehreren Krankenkassen angebotene Gesundheitsapp Vivy setzt auf dieses Prinzip. Hier wird das Benutzerkonto neben einem Passwort fest an das verwendete Smartphone gekoppelt. Die Authentifizierung erfolgt per SMS und ist Basis für die Verschlüsselung zwischen Patient und Arztpraxis.

Die Zwei-Faktor-Authentifizierung steigere die Sicherheit maßgeblich, sagt Olivier Perroquin, Geschäftsführer von In-Webo, einem Anbieter von Sicherheitstechnologie. „Allerdings scheuen viele digitale Dienste dennoch die konsequente Umsetzung dieses Prinzips." Denn sind Codegenerator, Smartphone oder Token gerade nicht zur Hand, ist eine Anmeldung nicht möglich.

Zudem möchten manche Unternehmen ihr Kunden nicht mit einem komplizierteren Anmeldeprozess belästigen. Daher habe In-Webo einen Mittelweg entwickelt, der auf ein zusätzliches Gerät verzichtet, aber ein vergleichbares Schutz niveau erzielt, indem zwei unterschiedliche Sicherheitsfaktoren über den Webbrowser des Nutzers bereitstellt werden.

Besserer Schutz im Webbrowser

Dazu meldet sich der Anwender mit den vom Anbieter zugesandten Zugangsdaten auf seinem üblicherweise genutzten Computer beim Dienst an. Der Nutzer erhält dann nur eine Identifikationsnummer, er muss aber keinen Namen oder andere persönliche Daten angeben. Erst auf der Gegenseite, etwa in Arztpraxis oder Klinik, erfolgt dann die Verknüpfung zwischen ID und persönlichen Daten. Für die Verschlüsselung und Authentifizierung muss der Kommunikationspartner jedoch keine Spezialsysteme vorhalten, die nötige Infrastruktur betreibt In-Webo in seinen Firmengebäuden.

Die Lösung sei für die Nutzer genauso komfortabel wie eine einfache Anmeldung. Gleichzeitig biete sie zuverlässigen Schutz gegen Angriffe wie Phishing (E-Mails mit Schadprogrammen) oder manipulierte Webseiten („HTML injection"). Und sie ist ohne Installation gleichermaßen auf PCs, Tablets und Smartphones nutzbar.

Hannes Rügheimer