Trickkiste Biometrie

Dass die Digitalisierung so nachhaltig von Rückgriffen auf analoge Werte und Verhaltensweisen beeinflusst wird, war vor zwanzig Jahren kaum abzusehen. Gemeint ist hier der Umgang mit Merkmalen, die traditionell das Erkennen und Wiedererkennen von Individuen ermöglichen. Diese öffentlichen – von jedem benutzbaren und prinzipiell nicht schützbaren – Werte sind zunächst analog. Ebenso werden die dazugehörenden Parameter (klein – groß, hell – dunkel, schlank – gedrungen usw.) verwendet. Das Besondere ist, dass meist unmittelbar im Erkennungsprozess auch das Verhalten des beobachteten Individuums ebenfalls als Kriterium für die Erkennungssicherheit verwendet wird. Was im Leben so einfach erscheint, wird bei der Gestaltung von sinnvollen Anwendungen in der IT-Welt äußerst komplex. Die sichere Identifikation oder eine vertrauenswürdige Authentifikation mittels biometrischer Merkmale eines Individuums schienen zunächst plausible Ziele zu sein. Es gab ja einen riesigen Erfahrungshintergrund: das Passwort mit dem die genannten Aufgaben scheinbar ausreichend erfüllbar sind. Sofort fallen dabei aber konzeptionelle Schwachstellen auf. Die Sicherheit von passwortgestützten Anwendungen wird entscheidend davon geprägt, dass ein Geheimnis von seinem Besitzer sicher bewahrt und sorgfältig angewendet wird. Hier scheint die erste Barriere für die sinnvolle Anwendung von biometrischen Merkmalen in IT-Anwendungen auf: wie transformiert man einen öffentlichen Fingerabdruck oder ein Gesichtsbild in ein ausschließlich individuell verfügbares Geheimnis?

Diese Frage hat die Biometrie Enthusiasten viele Jahre beschäftigt. Die Antwort besteht ganz allgemein im Wandel der einmaligen analogen biometrischen Bilder in digitale Templates und deren Anpassung an Anforderungen, wie man sie zum Beispiel von Passworten kennt. Mit diesem Schritt sind biometrische Merkmale dann den Algorithmen und Programmen unterworfen, die zu ‚Geheimnissen' in der IT-Welt gehören. Allerdings werden damit auch alle Schwachstellen von und Angriffsszenarien gegen kryptografische Verfahren und deren erforderliche Infrastrukturen vererbt. Insofern wird bei der Verwendung von Templates biometrischer Bilder im Allgemeinen auch kein höheres Sicherheitsniveau als in der Passwort-Welt erreicht.

Entscheidend für die praktische Verwendbarkeit von biometrischen Merkmalen ist und bleibt ihre zielgerichtete Transformation in ein Template. Dabei sind spezifische Anforderungen zu erfüllen, die in der Natur der Sache liegen. Die biometrischen Merkmale sind per Definitionem unveränderbar und sind selbst kein Geheimnis, sie dürfen unter keinen Umständen aus den Template-Daten zurückgewonnen werden. Weil die lebende Natur Ursprung der biometrischen Charakteristika ist, wird auch eine ausreichende Fehlertoleranz benötigt. Aus diesen Gründen beruhen die Lösungen für die Template-Berechnungen auf meist nicht öffentlichen (proprietären) Algorithmen und sind auch an eine spezifische Sensorik gebunden.

Beeindruckend sind jedenfalls die erreichten Anwendungsqualitäten: sowohl Fingerprint als auch Gesichtserkennung haben feste und akzeptierte Positionen als ausreichend sichere und anwenderfreundliche Methoden des Entsperrens von Mobilgeräten erreicht.

Mit herzlichen Grüßen, Ihr

Ihr Helmut Reimer