TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

05.09.2012

Positionspapier der TeleTrusT-Arbeitsgruppe "Biometrie" (Version 2)

Regelung des Biometrie-Einsatzes in der Arbeitswelt

Der Bundesverband IT-Sicherheit (TeleTrusT) unterstützt seit über 20 Jahren die Schaffung verlässlicher Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik. Mit über 170 Mitgliedern aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen hat TeleTrusT ein Kompetenznetzwerk geschaffen, das auch im Bereich Biometrie europaweit führend ist. Auf dem Gebiet der Biometrie, hier definiert als "automatisierte Erkennung von Individuen, basierend auf deren Verhaltens- und biologischen Charakteristika", arbeiten bei TeleTrusT die wichtigsten deutschen Hersteller und Anwender von Biometrietechnologie mit renommierten Forschern und Entwicklern interdisziplinär zusammen.

Als hochwertiges Authentifizierungsmittel sind biometrische Systeme gerade auch für den Einsatz in der Arbeitswelt prädestiniert. Aufgrund der besonderen Natur biometrischer Daten hat insbesondere das Unternehmen als Betreiber eine besondere datenschutzrechtliche Verantwortung für seine Mitarbeiter als "Betroffene" (im Sinne der Datenschutzgesetze).

TeleTrusT steht dem Einsatz der Biometrie zu Authentifizierungszwecken grundsätzlich bejahend gegenüber. Biometrische Systeme können dem Betreiber Sicherheits- und Kostenvorteile bieten und den Betroffenen eine komfortable Authentifizierung ermöglichen. Dies setzt jedoch neben einem verantwortungsvollen Umgang der Betreiber mit den biometrischen Daten auch die Kooperationsbereitschaft der Betroffenen voraus. Nur wenn die Betroffenen von den Vorteilen des biometrischen Systems überzeugt werden konnten, kann der für den Betreiber erwartete Nutzen eintreten.

Auf Grund der besonderen Natur biometrischer Daten sind diese als besonders schützenswert anzusehen. Dieses besondere Schutzbedürfnis folgt einerseits aus der Möglichkeit, Personen anhand von biometrischen Daten mehr oder weniger eindeutig zuordnen zu können. Damit lassen sich biometrische Daten ähnlich einem Personenkennzeichen nutzen, was im Widerspruch zu bisherigen Verfassungsgerichtsurteilen stehen kann.

Andererseits lässt sich nicht ausschließen, dass biometrische Daten besonders sensible persönliche Informationen enthalten, die über das hinausgehen, was zur Authentifizierung genutzt wird. TeleTrusT sieht es sehr kritisch, wenn Betreiber (evtl. auch heimlich) Auswertungen betreiben, die nicht im Interesse des Betroffenen stehen. Mit organisatorischen und technischen Maßnahmen ist bei der Speicherung biometrischer Daten sicherzustellen, dass diese nicht entwendet werden können und im Fall der Entwendung für den Betroffenen kein Schaden entstehen kann.

Zur besonderen Verantwortung des Betreibers eines biometrischen Systems gehört es, die biometrischen Daten keinesfalls an Dritte weiterzugeben. Angesichts des Wertes biometrischer Daten ist es Dritten durchaus zuzumuten, benötigte biometrischer Daten unter Mitwirkung des Betroffenen neu zu erfassen. Auf diese Weise kann der Betroffene selbst einen Überblick darüber behalten, wer über seine biometrischen Daten verfügt und sie verarbeitet.

Freiwilligkeit ist eine wesentliche Voraussetzung für die Akzeptanz biometrischer Systeme. TeleTrusT sieht die Gefahr, dass bei einem individuellen Zustimmungserfordernis nicht nur Mitbestimmungsrechte ausgehebelt werden, sondern die für das einwandfreie Funktionieren des biometrischen Systems erforderliche *echte* Freiwilligkeit auf der Strecke bleibt. TeleTrusT fordert deshalb bei der Einrichtung biometrischer Systeme im Arbeitsumfeld die Beibehaltung der bisherigen Mitbestimmungspflicht durch Arbeitnehmervertretungen und empfiehlt diskriminierungsfreie Alternativen, die aus biologisch-technischen Gründen für jede Art von Authentifizierung erforderlich sind. Für Mitarbeiter von Kleinunternehmen muss es möglich sein, sich vertraulich an Datenschutzaufsichtsbehörden wenden zu können, so dass diese Behörden - sofern notwendig - stellvertretend einen Einsatz in einem Unternehmen gestaltend im Sinne der betroffenen Mitarbeiter begleiten.

TeleTrusT spricht sich gegen eine überbordende Regulierung aus. Insbesondere ist es wenig sinnvoll, die Biometrie aus einzelnen Anwendungen wie Zeiterfassung auszuschließen oder auf Authentifizierungsanwendungen zu begrenzen. Gleichwohl hält es TeleTrusT für essenziell, auch bei weniger sicherheitsrelevanten Anwendungen höchste Standards beim Schutz der biometrischen Daten zu fordern. So wurde beispielsweise mit ISO/IEC 24745 "Biometric Information Protection" ein internationaler Standard etabliert, der einen Rahmen für bestmöglichen Schutz von Referenzdaten bietet, so dass ungewünschte Verknüpfungen vermieden und eine Rückrufbarkeit von biometrischen Referenzen ermöglicht werden.

Unterschiedliche Modalitäten biometrischer Charakteristika (Finger, Gesicht, Iris, Stimme, Tippverhalten etc.) können sich erheblich in Bezug auf ihre Datenschutzsensibilität unterscheiden. Dies kann biologische, technische und kulturelle Hintergründe haben. Um auch neuere Forschungsergebnisse oder gesellschaftliche Veränderungen berücksichtigen zu können, wird dringend empfohlen, von einer Regulierung einzelner Modalitäten abzusehen und stattdessen deren datenschutzkritischen Eigenschaften zu betrachten, um auf diese Weise zu allgemeingültigen Kriterien zu gelangen.

TeleTrusT fordert eine risiko- und technikadäquate Regelung. Für die Technikgestaltung könnte ein Rahmen gesetzt werden, wie dies die EU-Kommission bzw. die Artikel-29-Datenschutzgruppe (Arbeitspapier 180) bereits getan haben, der biometrische Anwendungen in der Arbeitswelt in Risikostufen einteilt. So können datensparsamere Anwendungen anders gewertet werden als Anwendungen, in denen Zweckänderungen und Missbrauch zu befürchten sind. Indem der Betreiber zur Vorabkontrolle verpflichtet wird, kann aus Herstellersicht ein Markt für datensparsame Anwendungen geschaffen und aus Betroffenensicht der grundrechtliche Datenschutz verbessert werden.

Biometrische Daten werden seit langem auch erfolgreich für Zwecke der Strafverfolgung eingesetzt. Es ist jedoch eine klare Trennung zwischen dem Einsatz in der Privatwirtschaft und der Nutzung für kriminalistische Untersuchungen zu fordern. Es sind alle staatlichen Maßnahmen zu vermeiden, die die Funktionsfähigkeit privatwirtschaftlicher biometrischer Systeme beeinträchtigen könnten. So darf es z.B. keine regulative Forderung geben, die biometrischen Daten eines privatwirtschaftlichen Systems entschlüsseln und herausgeben zu müssen, um sie z.B. Strafverfolgungsbehörden zur Verfügung zu stellen, da dies erhebliche Konsequenzen für die Sicherheit haben kann. Gleiches gilt für den verpflichtenden Einbau von "Hintertüren" oder Sollbruchstellen.

Sollten biometrische Daten nicht mehr zu ihrem vereinbarten Einsatzzweck gebraucht werden, sind sie inklusive der Backups unverzüglich zu löschen. Biometrische Daten sind immer durch Neuerfassung wiederherstellbar.

TeleTrusT setzt sich zum Zweck der Beseitigung von Markthemmnissen für die Harmonisierung von Datenschutzregelungen einzelner EU-Staaten ein.