# Anwendungsgebiete der Biometrie

Seminar Biometrie
SS 2004

Normen Rohde
163432

## *Abstract*

Die nachfolgenden 5 Kapiteln bilden den 1. Teil einer Ausarbeitung über aktuelle Einsatzgebiete der Biometrie. Nach einer Einführung in die gewählte Kategorisierung von Biometrieanwendung wird in den einzelnen Kapiteln auf folgende Aspekte eingegangen: gegenwärtiger Stand, Trends die sich abzeichnen, Kosten, biometrische Techniken die für das Einsatzgebiet geeignet sind und spezifische Problematiken die bei der Anwendung von Biometrie in diesem Bereich gelöst werden müssen.
Außerdem wird zu jedem Einsatzgebiet eine Matrix vorgestellt die eine realistische Einschätzung über die Notwendigkeit der Einführung von Biometrie unterstützt.

Im zweiten Teil wird der Einsatz von Biometrie in Kundenbeziehungen des Ebuisness untersucht und eine allgemeine Beschreibung der vertikalen Marktsegmente unter dem Gesichtspunkt des Einsatzes von Biometrie gegeben.

## *1. Einführung*

Während sich viele Menschen fragen welche Biometrietechnologi in einem bestimmten Marktbereich angewendet werden kann, ist die eigentlich viel interessantere Frage: Welche Aufgabe soll der Einsatz von Biometrie lösen ? Mit dieser Fragestellung vor Augen (auch als horizontaler Ansatz bekannt) lässt sich die Frage nach einem effektiven Einsatz von Biometrie leichter beantworten.
Eine Dichotomie der Biometrieanwendungen in die Bereiche logischer/physischer Zugriff oder Identifikation/Verifikation verdeutlicht einige grundsätzliche Unterschiede in der Anwendung von Biometrie. Allerdings werden mit dieser Aufteilung Biometrieanwendungen zusammengefasst die sich teilweise deutlich in den nachfolgenden Punkten unterscheiden:

a) Wie interagiert der Benutzer mit dem Biometrischen System ? Erfolgt die Interaktion unter Aufsicht ?
b) Gibt es anwendungsspezifische Anforderungen an Genauigkeit, Anmeldungsvorgang, oder Reaktionsszeiten des Systems ?
c) Verhält sich die zu identifizierende (verifizierende) Person kooperativ ?
d) Wie hoch ist der Wert der durch Biometrie geschützten Daten ?
e) Welche nichtbiometrischen Alternativen gibt es ?

Unter Einbeziehung der genannten Fragestellungen kristallieren sich sieben Bereiche heraus, in die sich biometrische Anwendungen aufteilen lassen:

In den Rollenbeziehungen Bürger/Staat

1. Verbrechensbekämpfung
2. Identifikation
3. Überwachung

In den Rollenbeziehungen Arbeitgeber/Arbeitnehmer:

4. PC und Netzwerkzugänge
5. Zutritt und Anwesenheitskontrolle

In den Rollenbeziehungen Unternehmen /Kunde

6. ATM
7. e-commerce

Diese Aufteilung rückt das Problem das mit Biometire gelöst werden kann stärker in das Zentrum der Aufmerksamkeit, als die konkrete Technologie die zur Anwendung kommen könnte. Auf mögliche Technologien wird in den einzelnen Kapiteln seperat eingegangen.

## *2. Biometrie in der Verbrechensbekämpfung*

Der Einsatz von Biometrie soll in der Verbrechensbekämpfung der eindeutigen Identifizierung oder Verifizierung von Verdächtigen oder Beschuldigten dienen.

Die Identifikation von mutmaßlichen Verbrechern ist das bis heute ausgeprägteste Einsatzgebiet von Biometrie. In den letzten 25 Jahren entstanden insbesondere in den USA nationsweite Datenbanken von Fingerabdrücken die eine automatisierte Suche ermöglichen.

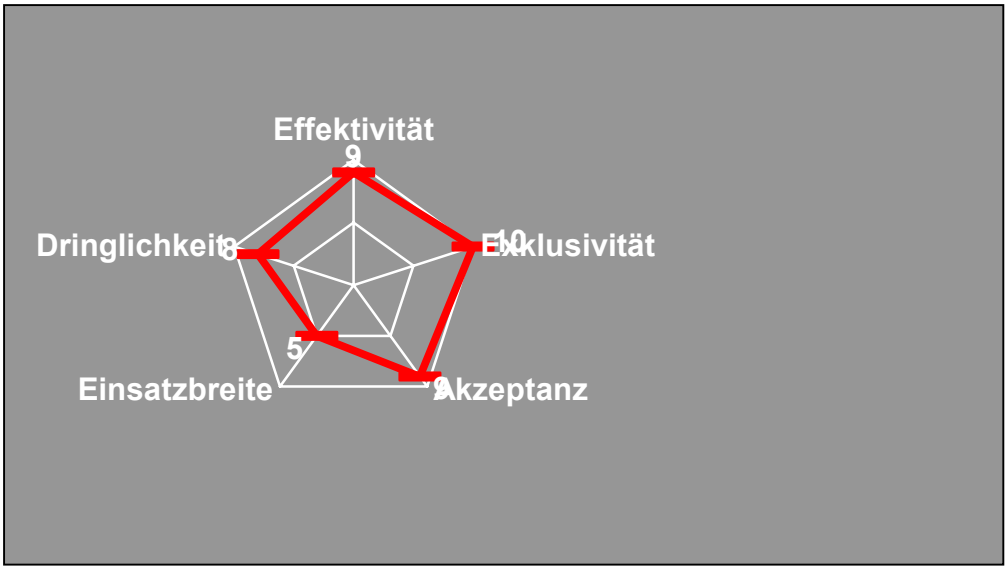
Das Wachstum in diesem Anwendungsgebiet wird hauptsächlich angetrieben durch die Entwicklung preiswerter Lösungen, insbesondere auch im Bereich der Lebenderkennung. Da es bereits große Datenbanken von Gesichtsaufnahmen gibt, erscheinen Technologien zur automatischen Identifizierung von Verdächtigen sehr attraktiv. Diese werden allerdings selten an die Genauigkeit von Systemen zum Abgleich von Fingerabdrücken heranreichen. Vorstellbar sind auch zukünftige internetbasierte Datenbanken die das internationale Wachstum automatisierter Zugriffsverfahren beschleunigen würden. Auch der automatisierte Zugriff auf DNA Datenbanken, die in den USA bereits aufgebaut werden, versprechen einen riesigen Effekt auf das Marktwachstum in diesem Bereich.

Neben den bereits erwähnten Technologien könnte sich Iris-Scan etablieren, die das Hauptproblem von Gesichtserkennung – die Genauigkeit - zu lösen scheint. Allerdings ist das Fehlen von Datenbanken ein Hemmnis für ein schnelles Wachstum in diesem Marktbereich.

Die Kosten für den Einsatz von Biometrie in der Verbrechensbekämpfung entstehen durch die Anschaffung von mobilen Endgeräten, Integration bereits vorhandener Lösungen, der Wartung von Hardware und Software. Insbesondere werden Systeme benötigt, die es ermöglichen tintenbasierte Fingerabdrücke präzise in die elektronische Datenverarbeitung zu überführen.

Zusammenfassend kann man sagen das der Bereich der Verbrechensbekämpfung von allen biometrischen Anwendungsfeldern die höchsten Reifegrad erreicht hat. In der Anwendung neuerer biometrischer Technologien (Gesichtserkennung, mobile Fingerabdrucksysteme) sollte der Hauptfokus in der langfristigen Zuverlässigkeit dieser Systeme liegen.

## *2.1 Empfehlungsmatrix*




Exklusivität (10): Biometrie ist die einzige Technologie die in der Lage ist eine eindeutigen Identifizierung sicherzustellen. Einzelpersonen mit falscher Identität können nur durch biometrische Daten korrekt identifiziert werden. Dadurch erklärt sich auch die hohe Reife die die Anwendung von Biometrie in diesem Bereich gegenüber anderen Einsatzgebieten gewonnen hat.

Effektivität(9): Obwohl es keine 100 %ige Fehlerfreiheit gibt, hat sich Biometrie als ein wirksames Mittel zur Identifizierung von Verbrechern erwiesen. Insbesondere Fingerabdrucksysteme mit Lebenderkennung bieten eine schnelle Identifizierung mit sehr hoher Genauigkeit. Größtes Hemmnis sind fehlende mobile Endgeräte.

Aufnahmebereitschaft(9): Es gibt wenig Widerstand bei der Anwendung von Biometrie zu Identifzierung von potentiellen Verbrechern. Es wird heute als notwendiger Bestandteil akzeptiert das Fingerabdrücke aufgenommen werden. Biometrie wird als notwendige Technologie wahrgenommen bei der Bedenken bezüglich Privatsphäre untergeordnet werden. Lediglich der Aufbau von DNA Datenbanken wird in der Öffentlichkeit mit Skepsis verfolgt, insbesondere wenn es um die Speicherung von Daten von Verdächtigen geht, die aber bisher keines Verbrechens überführt werden konnten. Die jüngsten Erfolge in Deutschland (Mordfall Mooshammer) sollten aber auch in der Öffentlichkeit zu einer verstärkten Akzeptanz führen.

Dringlichkeit(8): Die biometrische Identifizierung erscheint nicht immer als dringend notwendig da viele betreffende Personen auch ohne Biometrie korrekt identifiziert werden können. Trotzdem gibt es Situationen in denen die schnelle und zuverlässige Identitätsüberprüfung sehr wichtig ist, beispielsweise um eine Person in Gewahrsam zu halten.

Anwendungsbreite(5): Die meisten Menschen werden selten in die Verlegenheit kommen sich aus Gründen der Verbrechensbekämpfung einer biometrischen Zwangsidentifikation zu unterziehen. Da ein täglicher Kontakt mit diesem Anwendungsgebiet somit nur einen kleinen Teil der Bevölkerung betrifft, ist der Anwendungsbereich beschränkt.

## *2. Biometrie in der Bürgeridentifizierung*

In diesem Anwendungsgebiet wird Biometrie eingesetzt um die Identität von Einzelpersonen gegenüber dem Staat zu verifizieren. Mögliche konkrete Einsatzgebiete sind Wahlen, Kartenausgabe, Einwanderung, Sozialleistungen, oder die Überprüfungen von Beschäftigungsverhältnissen.

In Uganda wurden bereits bei Wahlen in 2001 Gesichtserkennungssysteme eingesetzt um Mehrfachwähler abzuhalten. In den USA setzen eine Reihe von Bundesstaaten die Abgabe von Fingerabdrücken zum Bezug von Sozialleistungen voraus. Auch für die einwanderungsrelevante Identifizierung oder der Ausgabe von Führerscheinen wird Biometrie in verschiedenen Staaten bereits eingesetzt.

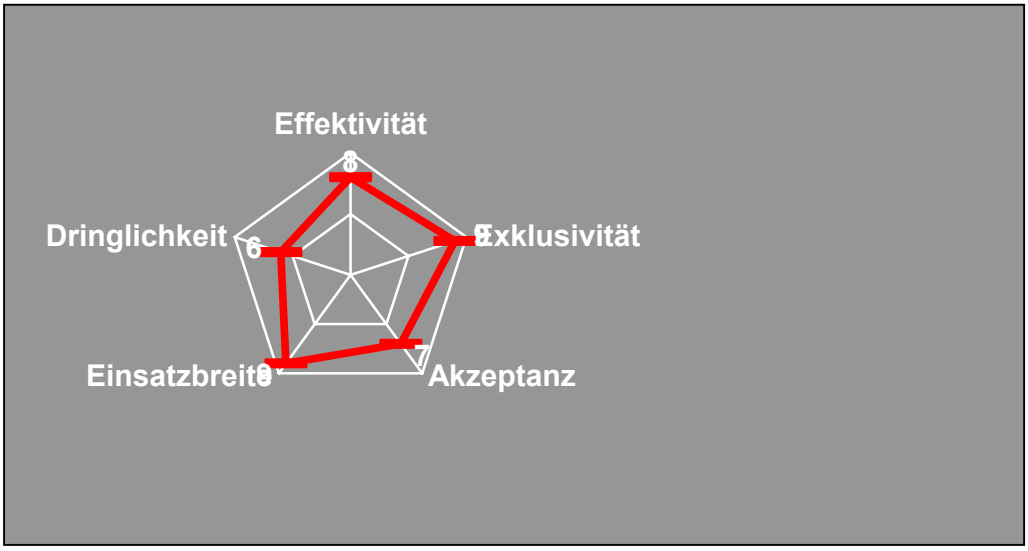
Der Einsatz von Biometrie wird besonders in den Bereichen stark vorangetrieben wo eine sichere Authentifizierung von Bürgern unbedingt notwendig ist um Missbrauch zu verhindern. Dies betrifft insbesondere den Erhalt von Sozialleistungen oder die Stimmenregistrierung bei Wahlen. Viele Anwendungen in der Bürgeridentifizierung setzen eine zentrale Datenbank zur effektiven Anwendung voraus. Grundsätzlich bestehen in den westlichen Industrienationen in der Bevölkerung stärkere Bedenken über Missbrauchsmöglichkeiten solcher Datenbanken als in Asien oder den Entwicklungsländern. Es ist deshalb gut möglich das gerade in diesen Ländern solche Anwendungen einem stärkerem Wachstum unterliegen. Als ein weiteres Hemmnis muss der hohe logistische Aufwand genannt werden um Millionen von Bürgern in einem biometrischen Identifikationssystem zu registrieren.

Biometrietechnologien die in diesem Bereich zum Einsatz kommen dürften vor allem AFIS, Gesichtserkennung und der Fingerabdruck sein. Iris-Scan scheidet wegen der hohen Kosten für einen breiten Einsatz aus.

Es gibt sechs wichtige Themen die bedacht werden müssen wenn Biometrie zu Bürgeridentifzierung eingesetzt werden soll.
Registrierung: Weil die Datenbanken mehrere Millionen Einträge umfassen können, wird der Registrierungsprozess extrem komplex und kann sich über Jahre hinziehen.
Anpassungsfähigkeit: Bevölkerugswachstum, Zuwanderung oder auch der potentielle Zusammenschluss von Staaten erfordern eine skalierbare Datenbank.
Antwortzeiten: Da jede Verzögerung nicht nur den einzelnen Anwender betrifft sondern auch Auswirkungen auf Nachfolgeprozesse haben kann, ist eine effiziente Filterung der Datenbankeinträge nötig.
Fehlerraten: Entwickler müssen sicherstellen das die Fehlerraten der Systeme innerhalb akzeptabler Grenzwerte liegen. Während eine „false nonmatch Rate“ von 5% ggf. als akzeptabel angesehen werden kann (95 % aller Betrugsversuche werden erkannt) könnte eine „false Match Rate“ in dieser Größenordnung die Akzeptanz des Systems in Frage stellen.
Altsysteme: Die Integration von vorhanden Datenbanken zur Gesichtserkennung oder die Weiterleitung in Nachfolgesysteme könnte sich als problemetisch erweisen, da diese Systeme gegebenfalls nicht auf einen automatisierten Zugriff in dieser Größenordnung ausgerichtet sind.
Privatsphäre: Es existiert ein großes Missbrauchspotential, da die Daten zentralisiert gespeichert werden und einen großen Teil der Bevölkerung erfassen.

Bürgeridentifzierung mit Biometrie gehört zu den herausforderndsten aber auch vielversprechendsten Anwendungsgebieten. In Bereichen wo der Staat ein hohes Maß an Identitätssicherheit benötigt ist Biometrie der einzige Weg um Missbrauch effektiv zu verhindern.

## *2.1 Empfehlungsmatrix*




Exklusivität(9): Biometrie ist die einzige Technologie die in der Lage ist viele der Funktionen die in der Bürgererkennung notwendig sind zu erfüllen.
Effektivität(8): Im Bereich der Finerabruckerkennung arbeiten viele Systeme sehr effektiv, allerdings gibt es gerade bei der Gesichtserkennung noch viel Forschungspotential.
Aufnahmebereitschaft(7): Die Aufnahmebereitschaft ist ein wichtiger Punkt bei der Einführung eines Systems das die Koopperationsbereitschaft der regierten (zumindest bei der Registrierung) benötigt. In den westlichen Ländern wird Biometrie oft nur für sehr spezifische Anwendungsbereiche akzeptiert. Es bleibt offen ob eine breite Einführung der biometrischen Bürgeridentifzierung angenommen wird.
Dringlichkeit(6): Da es funktionierende Altsysteme gibt und die Kosten für eine Neustrukturierung immens sind, ist Dringlichkeit der kritische Punkt.
Anwendungsbreite (9): Biometrie in der Bürgeridentifizierung hat das Potential von einer breiten Masse benutzt zu werden. Der limitierende Faktor könnte die Regelmäßigkeit der Anwendung sein. Beispielsweise das nach einer einmaligen Registrierung, diese nur alle paar Jahre erneuert wird.

## *3. Überwachung*

Durch Biometrie soll festgestellt ob sich eine bestimmte Person an einem überwachten Ort aufhält. Biometrie soll hierbei die herkömmlichen manuelle Systeme (Monitore) ersetzen oder ergänzen.

Überwachung durch Kameras wird insbesondere in Kasinos allgemein eingesetzt und auch akzeptiert. Die öffentliche Bereitschaft Kameraüberwachung auch an anderen öffentlichen Plätzen (Flughäfen etc) flächendeckend anzuwenden ist durch die Ereignisse des 11.9.2001 stark gestiegen.

Wichtigster Wachstumsfaktor ist die Frage ob Daten, die aus Millionen bereits installierter Kameras gewonnen werden, genügend Qualität aufweisen um eine automatische Identifikation durchzuführen. Zur Zeit muss diese Frage klar verneint werden. Der Abschreckungseffekt ist bei Kameras der weitaus größere Einflussfaktor.

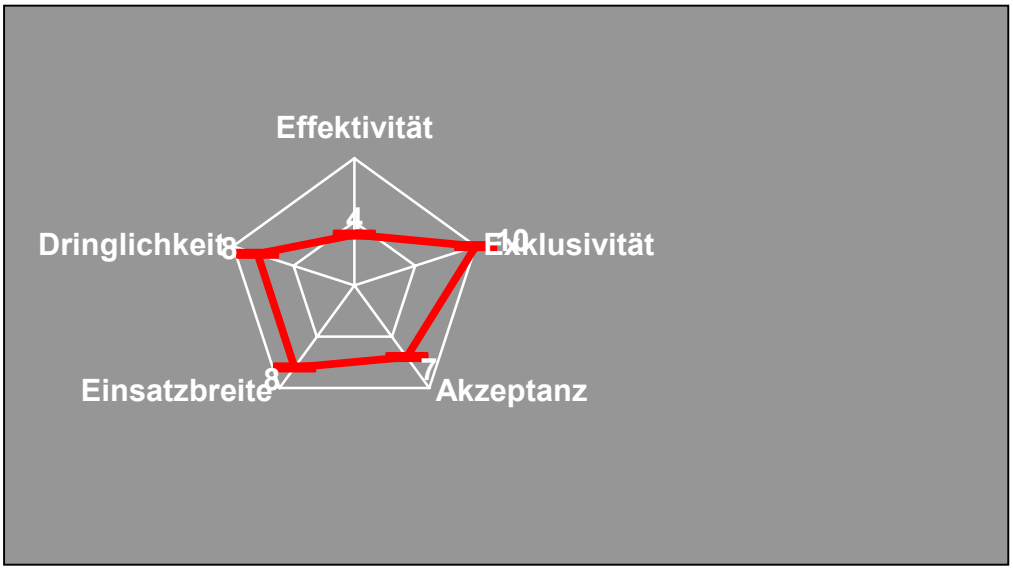
Gesichtserkennung ist zudem die einzige Technologie die zur Zeit überhaupt zur Überwachung eingesetzt werden kann. Es ist zwar möglich Stimmenerkennung zur reinen Verifikation zu nutzen, dieses wäre aber nicht die typische Anwendungsform im Sinne einer Überwachung. Technologien zur Stimmenidentifizierung unter mehreren Perosnen oder Identifizierung aufgrund von Bewegungsmerkmalen sind zur Zeit noch nicht entwickelt.

Die Kosten für Überwachungssysteme hängen stark davon ab ob die bisherige Kameratechnik Bilddaten von genügender Qualität liefert. Lizensgebühren für Gesichterkennungssysteme sind dann der primäre Kostenfaktor.

Folgende Themen müssen für die Einführung von Biometrie zur automatischen Überwachung bedacht werden:
Herkömmliche Kamerasysteme bieten selten eine Aufnahmequalität die für eine automatische Identifizierung nötig wäre. Einflussfaktoren wie Abstand, Winkel, Beleuchtung und Auflösung müssen auf das Foto abgestimmt sein auf Grundlage dessen eine Identifikation erfolgen soll.
Die meisten Gesichtserkennungssysteme nutzen zur Identifikation mehrere Fotos die während des Registrierungsprozesses aus verschiedenen Winkeln aufgenommen wurden. In Überwachungsszenarien gibt es oft nur ein einziges Foto mit geringer Qualität.
Wie bei allen anderen biometrischen Systemen gibt es keine 100% Sicherheit bei der Identifizierung. Es müssen deshalb Prozesse definiert werden die eine manuelle Überprüfung der Identität gewährleisten.
Während versteckte Kameras zwar besser vor nichtkooperativen Verhalten schützen (Maskierung etc) wird dadurch gleichzeitig der Haupteffekt, die Abschreckung, aufgehoben.

Zusammenfassend muss man sagen das Biometrie gegenwärtig noch keine effektiven Lösungen für die Überwachung anbietet.

### *3.1 Empfehlungsmatrix*




Exklusivität(10) Biometrie ist die einzige Möglichkeit automatisierte Überwachung durchzuführen. Dieser Punkt wird die Entwicklung auf diesem Gebiet weiter vorantreiben.
Effektivität(4) Die Effektivität kann nur im Abschreckungseffekt gemessen werden. Die Erkennung gesuchter Individuen ist mit der gegenwärtigen Technologie nicht wirksam durchführbar.
Aufnahmebereitschaft(7): Nach dem 11.September hat sich das öffentliche Bewusstsein zwischen Sicherheitsbedürfnis und Privatsphäre klar verschoben. Durch die erhöhte Forderung nach Sicherheit steigt auch die Anzahl der biometrischen Systeme die in der Überwachung zum Einsatz kommen.
Dringlichkeit(8) Bisherige Überwachungssysteme die der Aufdeckung von Taschendieben oder Kartenbetrügern dienten, erscheinen nebensächlich neben der Dringlichkeit Terroristen zu identifizieren.
Anwendungsbreite(8) Überwachungssysteme haben das Potential auf einem sehr breiten Einsatzgebiet zur Anwendung zu kommen. Wenn es gelingt bereits installierte Kamerasysteme in das neue System einzubinden hat dies einen starken Hebeleffekt auf die Einsatzbreite von biometrischen Überwachungssystemen.

## *4. PC und Netzwerkzugänge in Firmen*

Biometrie soll in diesem Bereich dazu dienen herkömmliche Authentifizierungsmechanismen wie Passwörter oder Schlüssel zu ersetzen. Dieser Bereich würde nach der klassischen Kategorisierung in den logischen Zugang fallen. Oft soll nur eine biometrische Verifizierung vorgenommen werden, da sich die Personen bereits durch andere Mechanismen identifiziert haben.
Der breite Einsatz von PC, Notebook, PDA und der steigende Wert von Informationen die über das Unternehmensnetz oder das Internet zugänglich sind, vergrößern das Bedürfnis nach einer sicheren Authentifizierung des Endbenutzers.

Es existieren bereits verschiedene Hardwarelösungen zur biometrischen Verifikation am PC, die hauptsächlich auf Fingerabdrücken basieren. In den letzten Jahren haben einige Firmen begonnen diese Technologie für den logischen Zugang ihrer Angestellten zu nutzen: im Januar 2001 begann beispielsweise die Stadt Glendale in Kalifornien mit der Aufrüstung ihrer Hardware auf biometrische Verifikation für 2100 Angestellte.

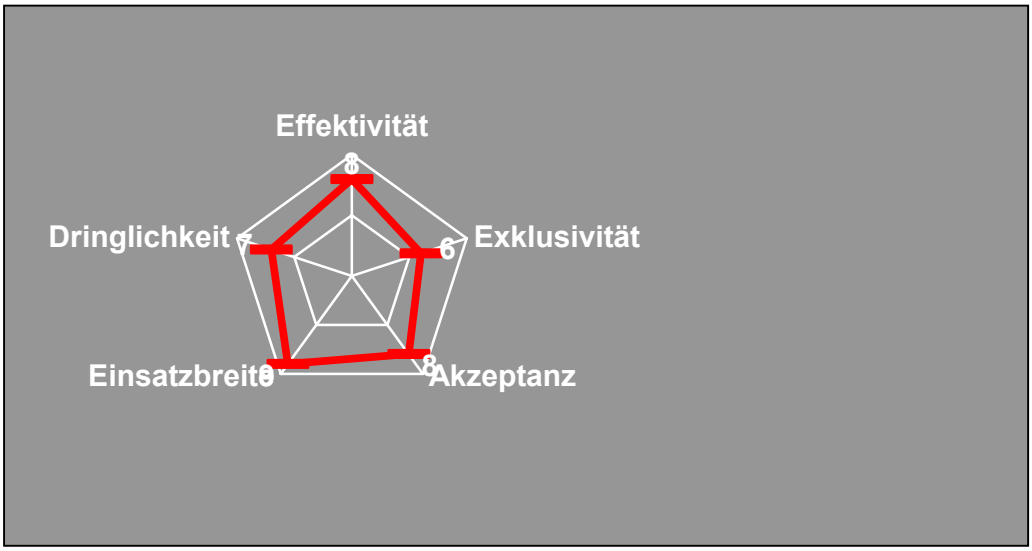
Die biometrischen Verifikation bei PC und Netzwerkzugängen steht aus den bereits genannt genannten Gründen vor einer steilen Wachstumskurve. Insbesondere das Bedürfnis sensible Daten jederzeit nur authentifizierten Nutzern zugänglich zu machen ist ein starker Motor für Entwicklungen in diesem Bereich. Auch der Abschluss von Standardisierungsbemühungen in der Biometrie (BioApi, Bapi, CBEFF) wird die Entwicklung vorantreiben. Biometrie steht in diesem Bereich in engem Zusammenhang mit Smartcards und der Anwendung von Public Key Infrastructure (PKI). Während PKI das System authentifiziert, wird der Nutzer duch Biometrie authentifiziert. In Smartcards soll Biometrie die bisherige Verifikation über PIN`s ersetzen. Der steigende Einsatz von Smartcards oder PKI vergrößert auch den Markt für biometrische Lösungen. Insbesondere in Deutschland könnten allerdings Datenschutzbedenken biometrische Lösungen als weniger attraktiv erscheinen lassen.

Zur Zeit wird nur der Fingerabdruck in größerem Stil zur Verifikation von Endusern eingesetzt. Alternative Technologien mit Stimmenerkennung und Gesichtserkennung erweisen sich als schwierig wegen starker Schwankungen bei Hintergrundbeleuchtung oder Hintergrundgeräuschen. Iris Erkennungssysteme kommen wegen der hohen Anschaffungskosten für einen breiten Einsatz an vielen Geräten nicht in Betracht.
Selbst zu den relativ geringen Hardwarekosten bei einer Verifikation mit Fingerabdruck, kommen Lizensgebühren für die Software zum Matching des Fingerabdrucks. Mögliche Geschäftsmodelle könnten auch den bestehenden Trend zum Outsourcing nutzen und den Authentifizierungsprozess auf externe Unternehmen auslagern, denen dann eine monatliche Gebühr für die Bereitstellung von Hard und Software gezahlt wird.

Vor der Anwendung von Biometrie muss das Unternehmen folgende Fragen klären:
Wie und Wann soll der Registrierungsprozess erfolgen ?
Werden die Endbenutzer an einem Arbeitsplatz bleiben oder muss sich der gleiche Endbenutzer in verschiedenen Räumen oder Endgeräten anmelden können ? Dies macht eine zentrale Authentifizierung notwendig.
Werden Remote Zugänge in das Firmennetz benötigt ? Es existieren bereits Notebooks die eine biometrische Verifikation auf dem CMOS Level anbieten, damit unberechtigte Nutzer den Bootvorgang nicht einleiten können.
Welche Fallback Routinen sind vorstellbar für Nutzer die aufgrund körperlicher Einschränkungen nicht an der biometrischen Verifizierung teilnehmen können ?
Wie wird das System den Benutzern vorgestellt ? Nur eine informierte und kooperative Belegschaft kann die Systemeinführung erfolgreich werden lassen.
Welcher Aspekt soll im Vordergrund stehen: Wenige Abweisungen (geringe False Rejection Rate) oder wenige Fehler bei der Zutrittsgewährung?

Biometrie in der logischen Zugangsgewährung wird wahrscheinlich der erste große Bereich sein, in dem Biometrie vielen Menschen täglich begegnet. Da es auch Bestrebungen bei Microsoft und Intel gibt biometrische Verifikation in ihre angebotenen Produkte zu integrieren wird das Anwendungsrisiko für Unternehmen immer geringer, denn Standard Software und Hardwareprodukte besitzen häufig mehr technologische Reife als Individuallösungen.

## *4.1 Empfehlungsmatrix*




Exklusivität(6): Da es bereits viele alternative Systeme gibt die eine logische Zugangskontrolle anbieten (Passwort, Schlüssel, Karten) ist diese Frage der limitierende Faktor.
Effektivität(8): Da die Fehlerraten insbesondere bei der Verifikation mit Fingerabdruck sehr niedrig sind, und sich diese Systeme gut in bereits bestehende Authentifizierungsprozesse einbinden lassen, gilt Biometrie als eine effektive Lösung.
Aufnahmebereitschaft(8): Grundsätzlich kann eine hohe Bereitschaft angenommen werden, da Biometrie mehr Sicherheit bei mehr Komfort (vgl Passwort) anbietet. Voraussetzung ist allerdings eine über die Gründe der Einführung gut informierte Endbenutzergruppe.
Dringlichkeit(7): Obwohl bisherige Systeme auch ohne Biometrie jahrelang effektiv gearbeitet haben, gibt es wie bereits beschrieben eine steigendes Bedürfnis nach mehr Sicherheit.
Anwendungsbreite(8): Biometrische Lösugnen für den PC und Netzwerkzugang haben das Potential bald das tägliche Leben im Arbeits und Privatbereich zu prägen.

## *5. Zutrittskontrolle / Zeit und Anwesenheitsüberwachung*

Biometrie soll eingesetzt werden um die Identität einer Person zu identifizieren während diese ein Gebäude oder einen Raum betritt. Herkömmliche Authentifizierungsmechanismen wie Karten etc sollen dadurch ersetzt werden.

Bereits seit einigen Jahren gibt es Sicherungssysteme die über einen Fingerabdruck den Zutritt zu Räumen gewähren. Insbesondere im Militär, Kraftwerken oder bei Banken stehen drängende Gründe hinter einer biometrischen Verifikation. Zur Anwendung kommen biometrische Sicherungssysteme aber auch in diesen Bereichen nur in ganz bestimmten Räumen, da eine Absicherung aller Türen mit Biometrie nicht praktikabel erscheint. Aber auch in der Anwesenheitskontrolle können biometrische Systeme den Unternehmen viel Geld sparen, da sich Betrugsfälle wirksam verhindern lassen.

Wichtigste Faktoren für das Zukünftige Vordringen von Biometrietechniken in diesem Bereich ist die Vereinfachung der Nutzung und reduzierte Anschaffungskosten.
Ein Hemmnis für das Wachstum sind die geringen Stückzahlen die für eine Installation benötigt werden. Da ein Gerät sehr vielen Anwendern zur Verifikation dient, muss der Arbeitgeber zwar nur wenige anschaffen diese sind dafür aber umso teurer, da sich für Anbieter dieser Systeme keine Skaleneffekte ergeben.
Desweiteren konkurriert Biometrie in diesem Bereich mit verschiedenen Technologien (z.B. Zugangskarten) die sich seit Jahren als effektiv erwiesen haben.

Handerkennung und Fingerabdruck waren in den vergangen Jahren die üblichen Technologien um mit Biometrie Zutrittskontrollen zu gewährleisten. In Hochsicherheitsbereichen gibt es auch einige Anwendungsbeispiele für Retina Erkennung und Iris Erkennung.

Die Kosten enstehen hauptsächlich für die Integration der Hardware in die bestehende Gebäudesicherheitstechnik und variieren stark in Bezug auf die Anzahl der zu installierenden Systeme. Zu beachten ist auch ob an den bestehenden Türsystemen große bauliche Veränderungen vorgenommen werden müssen. Softwarelösungen die eine zentrale Userverwaltung ermöglichen sind mit teilweise unter 1000 EUR für Unternehmen relativ preiswert erhältlich.

Bei der Einführung von Biometrie zur Zutrittskontrolle und Anwesenheitsüberwachung müssen einige spezifische Aspekte berücksichtigt werden, die nachfolgend aufgeführt sind.

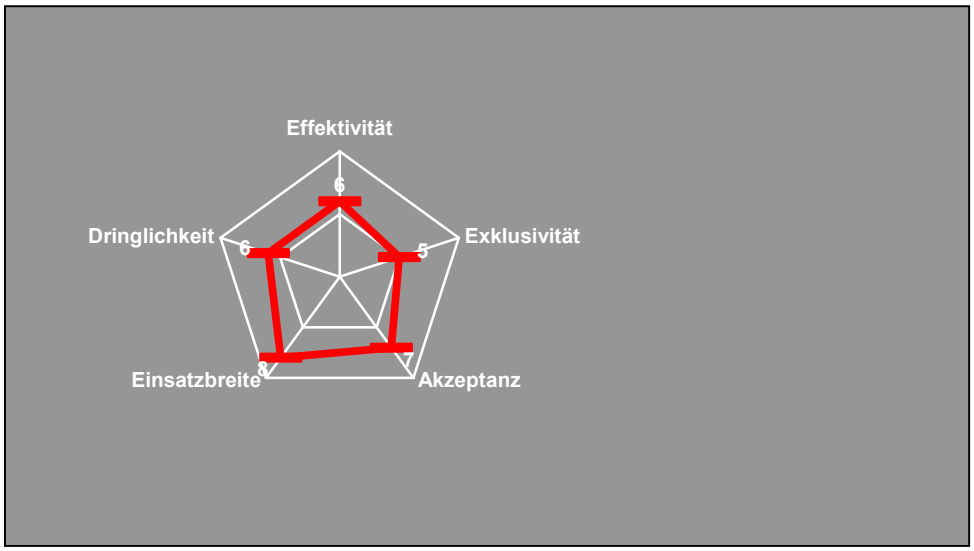
Wenn das bisherige Zutrittskontrollsystem sehr einfach zu benutzen ist, könnte dies zu einer mangelnden Akzeptanz bei den Angestellten führen, insbesondere wenn das biometrische System im Verifikationsmodus angewendet wird (d.h. es ist noch eine zusätzliche Identifizierung notwendig).

Das biometrische System sollte auch zu Höchstbelastungszeiten (Schichtechsel im Betrieb o.ä.) in der Lage sein, die Verifikation/Identifikation schnell und ohne Wartezeiten abzuwickeln. Engpässe in diesem Bereich könnten dazu führen das die Nutzer versuchen das System zu umgehen (offene Türen etc).

Es muss geklärt werden welche Fallback Prozeduren in Frage kommen, da es immer einen bestimmten Prozentsatz an Nutzern gibt, für die eine biometrische Identifizierung/Verifikation aus körperlichen oder anderen Gründen nicht möglich ist.

Zusammenfassend muss man sagen, das das Wachstum der biometrischen Zutrittskontrolle kaum mit dem schnellen Wachstum in der biometrischen  logischen Zugangskontrolle zu vergleichen ist. Allerdings gibt es für den Bereich der Zeit und Anwesenheitsüberwachung durchaus einige bereits genannte Punkte die ein weiteres Vordringen der Biometrie in diesem Bereich ermöglichen können.

## *5.1 Empfehlungsmatrix*




Exklusivität(5): Durch die bereits etablierten Alternativmöglichkeiten bei der Zutrittskontrolle (Karten, Schlüssel...)ist Exklusivität der limitierende Faktor. Auch wenn diese Varianten leichter übertragbar sind, und damit die Sicherheit des ganzen Systems gefährden, ist die Anwendung oft unkomplizierter als der Einsatz von Biometrie. In der Anwesenheits~ und Zeitkontrolle könnte Biometrie schon eher alte Systeme verdrängen da nur durch Biometrie das Problem von Betrugsfällen (z.B. Zeitkarten werden vom Kollegen gezogen) wirksam verhindert werden kann.

Effektivität(6): Solange die Geschwindigkeit des Verifikationsvorgangs unerheblich ist, lösen biometrische Systeme Authentifizierungsprobleme. Gerade für große Menschenmassen (Schichtwechsel...) benötigt die Bereitstellung der biometrischen Daten und die oft zusätzlich notwendige Identifizierung (durch Pin o.ä.) zu viel Zeit.

Aufnahmebereitschaft(7): Der Einsatz von Biometrie in der Zutrittskontrolle wird wahrscheinlich eine höhere Aufnahmebereitschaft unter den Mitarbeitern vorfinden als bei der Anwesenheitskontrolle, da man vermuten kann das ein stärkeres Überwachungssystem durch das Verhalten einiger Mitarbeiter notwendig geworden ist. Die Akzeptanz hängt stark davon ab wie benutzerfreundlich und zuverlässig das biometrische System im Vergleich zu der bisherigen Lösung arbeitet.

Dringlichkeit(6): Durch die zunehmende Terrorgefahr und auch der zunehmenden Gewalt an Schulen steigt die Dringlichkeit für sichere Zutriitskontrollen an sensiblen Plätzen.

Anwendungsbreite(8): Das breite Marktpotential wo Biometrietechniken in der Zutrittskontrolle und der Anwesenheitsüberwachung zum Einsatz kommen könnten, bildet den stärksten positiven Faktor in der Empfehlungsmatrix. Es gibt unzählige Anwendungsszenarien wo Biometrie in Unternehmen für diesen Zweck eingesetzt werden könnte.

## *Literaturangaben*

„Biometrics"  Samir Nanavati, Michael Thieme, Raj Nanavati, 2002

Studie Sparkassenverlag

Studie Bundestag