Nr. 75 | Juni 2005

Schwerpunkt-Thema:

Biometrie

Inhaltsverzeichnis

Editorial 4

Biometrie – Les systèmes biométriques: des mots de passe « anatomiques » 5

Biometrie – Biometrische Systeme: Der Körper als Passwort 11

Biometrie – Biometric ID Card Debates 16

Biometrie – Die Zukunft gehört der Biometrie 20

Biometrie Sind biometrische Systeme teuer, aber sicher? 21

Corporate Governance – How the culture of an organisation affects Governance 24

Interviews 25

The ISACA Crossword Puzzle 26

In eigener Sache 27

Express Line 28

DACH-News 29

Veranstaltungen 33

Vereinsadressen 35

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich
mbretscher@kpmg.com

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni,
8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem ***NewsLetter*** nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Preise:
Mitglieder gratis
Abonnement CHF 35.–/Jahr
Einzelnummer CHF 10.–

Inserate:
1 Seite CHF 400.–
1/2 Seite CHF 240.–
1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Thema: Schnittstellenprüfung): September 2005, Redaktionsschluss: 5. August 2005

Editorial

An einem feuchten Sommertag, in einer dunklen Bar, traf ich mich vor einigen Jahren mit anderen Referenten nach einer Sicherheitskonferenz. In der grösstenteils müde oder sogar erschöpft wirkenden Runde stach eine Gestalt hervor – eine überdrehte Frau, welche voller Begeisterung über ihr neues Sofware- und Hardware-Produkt zur biometrischen Erkennung des Fingerabdrucks redete und kaum aufhören konnte.

Da ich mich schon damals im Rahmen meines CISA-Kurses und anderer Ausbildungen immer wieder mit der biometrischen Authentisierung beschäftigt hatte, stellte ich der Vertreterin die zentrale Frage zum Thema: „Was mache ich, wenn mir mein Fingerabdruck gestohlen wird?“ Ich kann heute nicht mehr sagen, ob ich die Frage irgendwann einmal im Unterricht von einem Kursteilnehmer gestellt erhielt, oder ob sie sich einfach so aus der ständigen Weiterentwicklung des Kursthemas herauskristallisiert hat – Tatsache aber ist, dass ich bis heute noch keine vernünftige Antwort darauf erhalten habe.

Im Unterricht stelle ich die Frage immer wieder: die am häufigsten gehörte Antwort ist, „… dann nehme ich einfach den nächsten Finger!“ Zwar provoziert diese Antwort die erwarteten Lacher. Vor allem, wenn man dann bildhaft beginnt, einen Finger nach dem anderen einzuklappen, sehen nämlich alle, dass dieser Lösungsvorschlag nicht wirklich zielführend ist.

Bei physischen und logischen Authentisierungsmerkmalen (***credentials***) kann ich bei einem Verlust, Diebstahl oder unautorisiertem Kopieren rasch reagieren: Das Schloss zum verlorenen Schlüssel lasse ich auswechseln oder den verlorenen Badge im Zutrittskontrollsystem sperren – und kein Dieb oder zufälliger Finder kann das mir abhanden gekommene physische Merkmal missbrauchen. Analog mit den logischen Merkmalen: Sobald ich merke, dass mir jemand beim Eintippen des Passwortes zugeschaut hat, kann ich dieses ändern; und für den Fall, wo ich dies nicht bemerkt habe, hilft mir ja der (hoffentlich) regelmässige Passwortwechsel weiter.

Was aber mache ich, wenn es einem Angreifer gelingt, z.B. wegen eines Design- oder Implementationsfehlers (oder wegen der anderen Unzulänglichkeiten der meisten biometrischen Systeme) mein biometrisches Merkmal so zu stehlen (d.h. zu kopieren), dass er es an meiner Stelle gebrauchen kann? Bei den biometrischen Zutrittskontrollsystemen der ersten Stunde wurden solche Angriffsszenarien als Schwächen früher Prototypen verniedlicht, welche bei der definitiven Version selbstverständlich behoben sind. Dann kam der vielzitierte Artikel in der Zeitschrift CT, wo die Redaktion die meisten der am Markt erhältlichen Systeme mit einfachsten Tricks überlisten konnte. Eine der witzigsten Reaktionen mehrerer (!) Hersteller war, die Redaktion hätte mit unfairen Mitteln ausserhalb der Designspezifikationen gekämpft (z.B. Klebestreifen, Pulver usw.) – als ob sich die Angreifer an das Benutzerhandbuch mit all diesen überflüssigen Hinweisen wie „Bitte nasse Katze nicht im Mikrowellenofen trocknen“ halten würden.

Ich empfehle allen Herstellern von Sicherheitsprodukten, sich mit „meinen“ CISA-Kursteilnehmern zu messen – was diese nicht selber herausfinden, holen sie über gezielte oder zufällige Recherche aus dem Internet. Vor wenigen Monaten erhielt ich ein Video des Chaos Computer Clubs, das in weniger als zwei Minuten die absolut perfekt funktionierende Methode zeigt, wie ich mit Sekundenkleber, Digitalkamera, hautfreundlichem Leim und anderen frei erhältlichen Hilfsmitteln innert Minuten eine perfekte Kopie des Fingerabdrucks einer beliebigen fremden Person herstellen und diese Kopie dann mit Erfolg zur Überlistung der biometrischen Zutrittskontrolle einsetzen kann. Realität und nicht eine Szene aus dem Kinofilm „Minority Report“!

Kommen wir zurück zu meiner Frage: Ich finde heraus, dass irgend jemand meinen Fingerabdruck „gestohlen“ und z.B. für die Einreise in ein anderes Land missbraucht hat. Wer glaubt, dass ich die Pass- oder Einwanderungsbehörden überzeugen kann, nicht ich sei an diesem Tag dort und dort eingereist und hätte dann diese oder jene Straftat verübt, soll das bitte einmal selber ausprobieren – der Wahn mancher Behörden im Zusammenhang mit biometrischen Merkmalen, z.B. in Reisepässen, wird das sicherlich zu einem reizvollen Erlebnis werden lassen (übrigens meine ich damit ausdrücklich auch die vielen „kleinen Brüder“ im europäischen Umfeld). Auch wenn man mit forensischen Methoden in gewissen Fällen nachweisen kann, dass der gefundene Fingerabdruck mit einer Kopie „gestempelt“ wurde und nicht einem echten Fingerabdruck entspricht, wird so etwas für die von mehreren Personen verwendeten Zutrittskontroll-/Registriersysteme (z.B. Einwanderungsbehörde, Schliessfächer, usw.) systembedingt nicht möglich sein.

Na ja – von all dem lese ich in den verschiedenen mir bereits vorliegenden Artikeln zum Schwerpunkt-Thema in diesem ***NewsLetter*** gar nichts. Und leider auch nichts zur zweiten Frage, welche mich seit Jahren beschäftigt: „Wenn ich das physische oder logische Authentisierungsmerkmal nicht mehr stehlen oder kopieren kann, weil die Unternehmen grundsätzlich nur noch biometrische Merkmale einsetzen – führt das dann nicht automatisch zu einer dramatischen Erhöhung des Risikos bezüglich Geiselnahme (man schleppt das Opfer zum Geldausgabeautomat) oder Körperverletzung (man amputiert mehr oder weniger freundlich den Körperteil, den man für den Zugang benötigt)?

Mit nachdenklichen Grüssen

Peter R. Bitterli, CISA

P.S.
Bitte die Artikel dennoch lesen – es lohnt sich!

Biometrie

Les systèmes biométriques: des mots de passe « anatomiques »

Les techniques traditionnelles d'authentification, comme les systèmes à mot de passe ou Smartcard, partent du principe que l'usager est détenteur d'un savoir confidentiel (vérification de l'identité par un savoir) ou qu'il est détenteur d'une « clé » personnelle matérialisée (vérification de l'identité à l'aide d'un document justificatif).

La biométrie, elle, met à contribution des caractéristiques physiologiques ou comportementales de l'usager à des fins d'authentification. C'est en ce sens qu'elle collecte non plus seulement des donnés corrélatives à l'individu (méthode exogène) mais des données qui lui sont inhérentes.

Les caractéristiques biométriques ont l'avantage de ne pas pouvoir être subtilisées et qu'elles ne peuvent être falsifiées que très difficilement. Il est également à considérer que, dans le cas de systèmes à mot de passe ou à carte à puce, on peut certes vérifier la validité de la carte ou de la clé, mais on ne contrôle pas si le détenteur-utilisateur est bien le détenteur légitime. Les moyens biométriques constituent une parade très efficace à ce déficit.

Tant au point de vue coût qu'en ce qui concerne leur efficacité, les méthodes biométriques peuvent représenter une alternative à d'autres systèmes de sécurisation, ou du moins en être complémentaires.

Les différences entre la vérification et l'identification

Dans le cas de l***'identification***, on confronte des données biométriques à un individu. Ceci implique une recherche dans une banque de données préalablement établie, et nous nous retrouvons donc ici dans la problématique des enquêtes policières. On appelle également cette méthode la comparaison ***« one-to-many »***.

Une ***vérification*** est par contre la démarche au cours de laquelle on doit démontrer à l'aide de moyens biométriques qu'une personne est bien celle qu'elle prétend être. C'est le cas de figure des contrôles d'accès, appelés aussi comparaison ***one-to-one***.

Mise en oeuvre de systèmes biométriques

Les systèmes d'authentification personnelle peuvent être utilisés partout ou des individus ont à décliner leur identité au moyen de systèmes techniques.

A SRG SSR idée suisse, ce sont:

- les limitations d'accès et le contrôle d'utilisateurs certifiés vis-à-vis d'informations sensibles de l'entreprise (données salariales par exemple) ou d'informations clients ou RH ;
- la limitation d'accès à des ressources informatiques (utilisation de l'Internet et de certaines applications) à un cercle de personnes donné ;
- l'amélioration de la sécurité des sites au moyen de mesures très sophistiquées de protection d'accès à des bâtiments, entrepôts, salles

informatique, bureaux intégrés à des immeubles publics, laboratoires ou systèmes sensibles ou encore aux équipements névralgiques d'unités de diffusion ;

Quelles sont les caractéristiques exploitables en biométrie ?

Les procédés d'identification profitent du fait qu'il existe différentes caractéristiques physiques et comportementales qui sont tout à fait propres à un individu unique. A l'aide d'un senseur, il est possible de déterminer ces caractéristiques et d'établir sans équivoque possible un lien envers cette personne.

L'anatomie humaine présente un grand nombre de données pouvant être mesurées. Certaines se présentent sous forme écrite dans notre passeport. Mais s'il s'agit de procéder automatiquement à un balayage et à une comparaison du résultat, les impératifs biométriques vont entraîner certaines contraintes que l'on peut résumer comme suit.

- Maintenabilité: la référence de mesure doit faire preuve de pérennité; elle ne doit pas se modifier sur un intervalle de temps prolongé ;
- Accessibilité: les caractéristiques exploitables doivent pouvoir être numérisables en un laps de temps bref ;
- Unicité: la caractéristique biométrique envisagée doit comporter suffisamment de traits pertinents pour assurer une différenciation vis-à-vis de tout autre individu ;
- Acceptation: les techniques de vérification de la caractéristique envisagée doivent pouvoir être cautionnées par un large public. Il conviendra par exemple d'exclure toute technique invasive, sollicitant certaines parties du corps et pouvant être (subjectivement) considérée comme une atteinte à l'intégrité corporelle ;
- Compactabilité: La collecte d'informations doit pouvoir être réduite à une quantité de données raisonnable et facilement maniable ;
- Fiabilité: le procédé doit présenter une bonne fiabilité et reproductibilité ;
- Confidentialité: il convient de pouvoir protéger la sphère privée de chacun.

Dans ces conditions, la quantité des caractéristiques pouvant être saisies de manière automatique – et qui ont toutes déjà fait l'objet d'une expérimentation – se trouve être réduite à la portion congrue. Le synoptique ci-dessous donnera un aperçu des conclusions qui ont jusqu'ici été tirées à leur sujet.

D'autres caractéristiques, comme par exemple le poids, la taille, la couleur des yeux ou des cheveux ainsi que d'autres signes particuliers devront être exclus car ne satisfaisant pas aux critères d'unicité, de saisibilité ou de maintenabilité.

Enregistrement et vérification

Les conditions préalables à la vérification d'un individu comportent la nécessité d'avoir enregistré la personne sous une référence XY dans le système de reconnaissance et que son signalement se soit matérialisé sous forme d'une entrée informatique comportant les informations biométriques.

Toute vérification biométrique commence pour cette raison par un enregistrement (capture de la référence). Nous l'illustrerons à l'exemple de l'empreinte digitale:

- choix d'un code d'identification individuel,
- présentation du doigt,
- numérisation de la configuration de l'empreinte,
- nouvelle présentation du doigt, test.

On vérifiera ensuite si la personne alléguant être la dénommée XY présente les caractéristiques biométriques correspondantes. Sont à cet effet requis:

1. la saisie de l'identité avancée par la personne.

Caractéristique	***Capture***	***Pérennité (maintenabilité)***	***Unicité***	***Acceptation***
Géométrie de la main	optique (IR)	bonne	1:1000	très bonne
Empreinte deux doigts	optique (IR)	bonne	1:1000	très bonne
Empreinte rétinienne	optique (laser)	très bonne	1: un million	médiocre (invasive)
Reconnaissance de l'iris	optique	très bonne	1: 6 millions	médiocre
Reconnaissance des veines de la main	optique	bonne	pas d'indication	très bonne
Signature	dynamique (pression exercée)	médiocre	1 : 10.000	très bonne
Caractéristiques vocales	électroacoustique	médiocre	1 : 10.000	bonne
Identification du visage	optique ou par IR	bonne	pas d'indication	bonne
Empreintes digitales	optique, capacitif etc.	très bonne	1 : un million	bonne

Tableau 1: Caractéristiques biométriques

2. L'interrogation de la banque de données comportant les indications sur cette personne.
3. La numérisation de ces données biométriques.
4. La collation des données informatiques et de la saisie personnelle.
5. L'affichage et le cas échéant le dépouillement des résultats.

Le traitement de l'image (« enrôlement ») et l'authentification peuvent s'effectuer de deux maniéres différentes.

Dans le premier cas, on opère l'extraction des minuties (terminaisons, bifurcations...) et on dépose les résultats dans une banque de données.

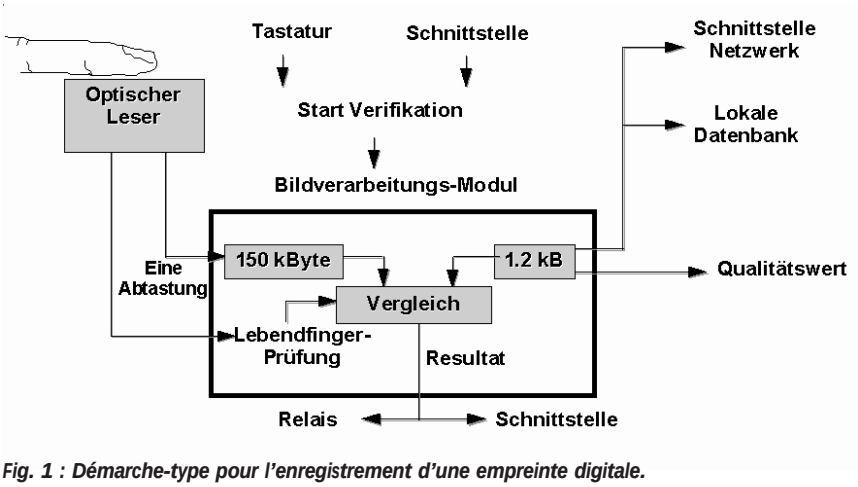


Fig. 1 : Démarche-type pour l'enregistrement d'une empreinte digitale.

Les caractéristiques biométriques et leur capture

Les empreintes digitales

Aujourd'hui la capture des empreintes digitales s'effectue par voie optique: le doigt est placé sur un prisme; au point de contact entre la peau et le prisme, la lumière fait l'objet d'une dispersion (et non d'une réflexion totale), et l'image qui en résulte va être reprise par une caméra CDD.

D'autres procédés de saisie ont été essayés, comme les méthodes aux ultrasons, les techniques capacitives ainsi que des méthodes combinées associant thermographie et pression. Le procédé aux ultrasons a été rejeté pour des raisons de coûts. Le procédé combiné en est encore au stade expérimental tandis que la méthode capacitive est d'ores et déjà utilisée.

Pour la vérification, on reprend les minuties de l'individu et effectue la comparaison avec les données enregistrées (« minutiae matching »).

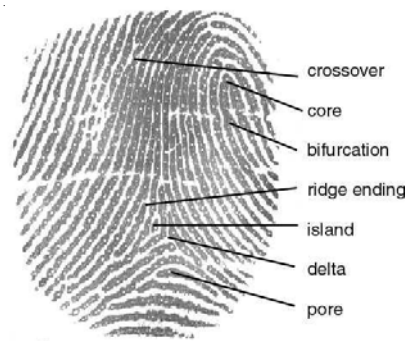


Fig. 2: Caractéristiques pertinentes d'une empreinte digitale

Dans le deuxième cas, on n'entre dans la base de données que certains éléments de l'image binarisée. De même, pour la vérification, on s'en référera au champ sélectionné de l'image binarisée pour vérifier la concordance avec la portion d'empreinte présentée (pattern matching).

On parvient dans les deux cas à un indice de similitude comparable, mais la durée de l'opération peut être supérieure dans le premier cas.

Rares sont les fournisseurs qui proposent une identification du doigt vivant, permettant d'exclure les authentifications d'une copie silicone ou, dans les cas extrêmes, les abus dans lesquels on aurait essayé de se légitimer au moyen du doigt d'une personne décédée.

Le visage

Il existe ici des procédés de reconnaissance visuelle et thermographique. Les traits caractéristiques d'un visage sont capturés au moyen d'une image vidéo.

Fig. 3: Reconnaissance d'un visage.

Plusieurs de ces procédés n'ont fait leur apparition que tout récemment. Utilisant un principe proche de la photographie, leur acceptation auprès des utilisateurs potentiels est particulièrement bonne. Combinés aux procédés requérant une capture oculaire, ils constituent une méthode absolument sans contact corporel.

Certaines réserves sans à émettre en ce qui concerne la protection des données informatiques. Ainsi, le procédé permet des investigations au sein d'une banque de données ou vice

versa pour la recherche d'un individu au sein d'un groupe. L'authentification de la personne peut en outre se faire à l'insu de celle-ci, ce qui est impossible par exemple pour les procédés digitaux ou palmaires. Citons à titre d'exemples pour une telle mise en oeuvre, délicate en termes des données, la surveillance des zones piétonnes ainsi que celle assumée par la police à l'encontre des supporters dans les stades britanniques.

L'iris et la rétine

Ces deux organes oculaires comptent parmi les plus fiables et les plus stables dans le temps; ils permettent même une différenciation satisfaisante chez les jumeaux monozygotes.

L'image de la pupille sera capturée soit par un laser « inoffensif » soit à l'aide d'une caméra vidéo. Après avoir binarisé la carte vasculaire et autres caractéristiques, on sauvegarde les données sous forme d'un code-barre.

Les obstacles inhérents aux techniques d'authentification oculaire consistent d'une part en la réticence des individus, et d'une part dans les problèmes de la capture, vu les différentes positions que les yeux peuvent avoir par rapport à l'appareil, ce qui implique une opération préalable de positionnement. On ne dispose pas encore, pour cette technologie, d'une expérience suffisante.

Comparaison des systèmes biométriques et des méthodes conventionnelles

Avantages

■ Contrairement aux techniques à carte, à badge ou à clé, les caractéristiques biométriques sont inaliénables et excluent toute possibilité de cession à des tiers.

■ Globalement, la plupart des caractéristiques entrant en ligne de compte sont suffisamment stables pour la durée de vie de l'individu au cours de laquelle une authentification peut s'avérer nécessaire.

■ Les possibilités de duplication sont faibles, malgré certaines fluctuations d'un procédé à l'autre. Les falsifications requièrent en règle générale un investissement important.

■ Les frais d'exploitation de tels systèmes sont modérés puisqu'il n'est pas à prévoir de gestion et de renouvellement de documents d'authentification (cartes, clés).

Inconvénients

■ L'investissement initial, notamment au niveau des équipements, est plus important que dans le cas de systèmes conventionnels.

■ L'intégrité de la personne peut, selon la caractéristique biométrique choisie et son exploitation, être mise en cause. Ceci prévaut notamment lorsque la démarche biométrique n'est pas seulement utilisée à des fins de vérification mais également pour l'identification de l'individu.

■ Certaines réserves sanitaires doivent être considérées.

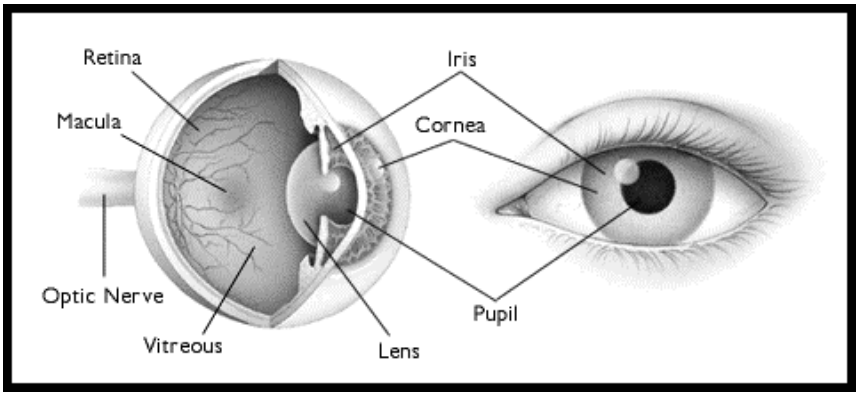


Fig. 4: Anatomie de l'oeil

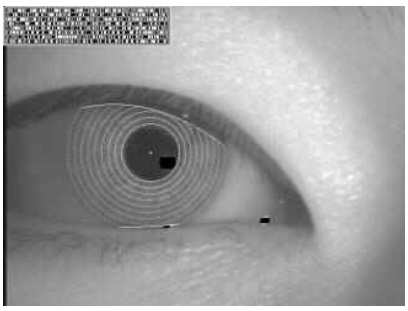


Fig. 5: Scannérisation de l'iris

Le marché

De manière générale, on constate que les systèmes biométriques peuvent être utilisés pour de très nombreuses applications. Ils présentent de nets avantages dans tous les cas où il est nécessaire d'identifier une personne avec la meilleure certitude possible. Le fait que ces systèmes ne soient pas plus utilisés est dû à plusieurs raisons:

■ cette technique est relativement récente. Cela fait seulement une quinzaine d'années que les premiers appareils ont été commercialisés; ils présentaient au début un encombrement dissuasif, ils étaient lents et leur prix était prohibitif. La conversion des structures existantes, souvent importantes (voir par exemple les équipements d'authentification aux guichets automatiques des banques) exigent d'énormes investissements, ce qui fait que les nouveaux systèmes ne s'imposent que progressivement.

■ Leur prix est encore élevé en comparaison, par exemple, à celui d'un lecteur de carte magnétique, quoique les prix soient appelés à baisser.
■ On avance souvent le problème de l'acceptation de la part du grand public, mais l'expérience montre que ce problème a tendance à être surestimé.
■ D'autre part, les lacunes qui subsistent dans le domaine de la normalisation amène la grosse clientèle potentielle de tels systèmes à temporiser, ceux-ci ne voulant pas être à la merci d'un seul et unique fournisseur.

Contrôles d'accès

De nombreux besoins peuvent être perçus dans ce domaine, qui dans le monde occidental, sont cependant uniquement appelés à faire office de complément à des systèmes existants et non à les supplanter.

Les systèmes biométriques connaissent une avancée significative, ces dernières années, pour la protection des casiers personnels dans les coffres-forts des banques, tant en Allemagne qu'en Suisse, et de plus en plus également en Autriche. Les systèmes mis en oeuvre se basent sur l'authentification digitale mais également sur les systèmes de reconnaissance du visage.

On rencontre en outre des équipements de contrôle d'accès biométriques dans les banques, les prisons, les centrales nucléaires, les installations militaires et de plus en plus également dans les industries et services.

A SRG SSR idée suisse, il serait envisageable de prévoir de tels systèmes pour la protection complémentaire des salles informatiques et des installations névralgiques de diffusion.

Protection des ordinateurs et des réseaux informatiques.

Le public averti sait bien que la protection de données par mot de passe, le moyen le plus utilisé actuellement, est dès plus problématique.

Si aucune mesure de dissuasion n'est prise, la majorité des utilisateurs fait appel à des mots de passe d'une dangereuse banalité, comme des prénoms ou des dates de naissance.

Si l'on procède à une exclusion délibérée, au niveau des logiciels, de combinaisons trop simples et si l'on impose un renouvellement plus fréquent du mot de passe ou du code personnel, les utilisateurs auront tendance à noter ces informations confidentielles et à les garder en un lieu peu sûr (tiroir de bureau, voire même souvent sur l'ordinateur même). Ceci est naturellement extrêmement dommageable à la sécurité.

Ces derniers temps, et du fait d'une baisse significative des prix, de plus en plus de systèmes d'authentification digitale ont fait leur apparition dans le domaine de la protection des ordinateurs. On perçoit donc dans ce domaine l'émergence d'un marché très important pour les systèmes biométriques.

Trois domaines d'application retiennent surtout l'attention:
1. La protection de l'accès aux ordinateurs eux-mêmes. Dans ce cas de figure, ce sont le démarrage de l'ordinateur ou encore l'accès aux systèmes d'exploitation installés (Windows NT par exemple), ou l'accès à certains répertoires se trouvant sur le disque dur qui seront bloqués.
2. L'interdiction de l'accès à des banques de données et de programmes sauvegardés sur les serveurs et requérant un code client. La protection de tels systèmes demande en plus la protection des informations véhiculées par le réseau.
3. Les signatures électroniques. Dans les cas où sont demandés des contrôles électroniques, par exemple pour des transactions pécuniaires par voie de réseau, les systèmes biométriques s'avèrent être particulièrement adaptés. Ici également, l'objectif visé est la protection de certaines opérations dans cet environnement « à hauts risques » que représente la Toile.

Dans l'état actuel des choses, l'utilisation de systèmes biométriques ne peut être envisagée à SRG SSR idée suisse que pour les deux premiers champs d'application, et ce en tant que modules complémentaires aux systèmes en place.

Acceptation

Préalablement à la mise en oeuvre d'équipements biométriques, il faut se pencher sur le problème de l'acceptation par les utilisateurs prévus. Il est à penser que surviendront par exemple des réserves d'ordre sanitaire pour les systèmes demandant un contact corporel.

Mais il sera bon de rappeler que nous touchons quotidiennement une multitude d'objets ayant été saisis avant nous par d'autres personnes (par exemple des poignées de porte), de sorte qu'il ne devrait pas y avoir de réticences envers des appareillages sensoriels sollicitant la géométrie de la main ou du doigt.

De manière générale, on peut constater que l'utilisateur ne verra aucun problème à ce genre de procédure – d'une fiabilité et d'une simplicité de manipulation convaincantes – pour autant qu'il ait été préalablement informé correctement.

Garantie de la confidentialité d'informations personnelles

La conservation de donnés biométriques affecte les droits individuels de la personne et présente ainsi une certaine pertinence en termes de protection informatique du citoyen. Ceci prévaut notamment pour les systèmes d'authentification de l'empreinte digitale, naturellement associée à des activités relevant du secteur policier.

Les systèmes ne se référant pas aux empreintes digitales ne donneront pas a priori lieu aux mêmes réticences, quoique la question de la protection de la confidentialité se pose ici avec la même acuité.

De l'avis des spécialistes de la protection informatique, la conservation de caractéristiques biométriques ne présente pas de problèmes tant qu'il s'agit d'une démarche délibérée de la part de l'utilisateur et que l'organisme instigateur joue la carte de la transparence.

Par ailleurs, tout acte d'authentification devrait être fonction de la volonté déclarée de la personne concernée, toute initiative prise à son insu étant donc à proscrire. A cet égard, les systèmes ne remplissent pas tous les conditions requises de la même manière. Les systèmes sans contact corporels (capture de l'image de l'iris ou du visage) donnent par exemple matière à controverse.

Particulièrement critiqués sont à cet égard les systèmes à empreinte digitale. Ces méthodes ne présentent pas de problèmes de protection tant que l'empreinte conservée ne permet pas de reconstituer la « signature » digitale. Si cette condition est remplie, les empreintes conservées ne sont pas utilisables à des fins policières et ne peuvent donc pas être utilisées sans la coopération de la personne concernée.

Les données biométriques ne présentent également aucun problème lorsqu'elles sont conservées non pas dans une banque de données mais sur une carte que l'utilisateur portera sur soit (carte de crédit par exemple).

La situation se présente différemment pour les systèmes permettant de procéder à une recherche dans une banque de données (principe « on to many »). Nous butons là aux limites qu'un organisme privé n'a pas le droit de dépasser. Ces questions dépendent néanmoins de la législation locale en vigueur. Les Etats-Unis par exemple concèdent à cet égard aux institutions privées beaucoup plus de latitude que ce n'est le cas en Europe.

Perspectives commerciales

Si l'on en croit les études effectuées par le Gartner Group et la International Biometric Industry Association (IBIA), on peut s'attendre à une avancée très rapide des systèmes biométriques.
En devenant d'une utilisation plus accessible et meilleure marché, et avec la réduction de leur encombrement, ces technologies ne supplanteront certes pas totalement les systèmes se référant à une propriété matérielle ou à un savoir (mots de passe, badge etc.), mais ils les remplaceront ou les compléteront partiellement dans de nombreux cas.

De la même manière que nous nous sommes habitués aux cartes magnétiques, aux cartes à puce et aux mots de passe, nous nous habituerons à la vérification biométrique. Le confort d'utilisation et la fiabilité des systèmes viendront sans nul doute à bout du scepticisme et apporteront la démonstration qu'il s'agit bien là de procédures d'identification somme toute bien naturelles.

Techniquement, la saisie de données biométriques recèle certains problèmes, ce qui veut dire qu'il conviendra de prévoir une dotation technique non négligeable si l'on veut garantir une fiabilité satisfaisante. Mais, dans le contexte d'une baisse généralisée du prix des composants électroniques et de la miniaturisation, ceci ne représentera pas une entrave insurmontable à l'extension de cette technologie. Le nombre des perspectives d'utilisation ira bien au contraire croissant.

Markus Gander, SRG SSR idée suisse, Berne

Biometrie

Biometrische Systeme: Der Körper als Passwort

Traditionelle Authentifikationstechniken, wie Passwort- oder Smartcard-Verfahren, beruhen darauf, dass der Teilnehmer über ein bestimmtes, nur ihm bekanntes Wissen verfügt (Verifikation der Identität durch Wissen) oder einen persönlichen Berechtigungsschlüssel besitzt (Verifikation der Identität durch Besitz).

Im Gegensatz dazu benutzt die Biometrie physiologische oder verhaltenstypische Charakteristiken des Teilnehmers zur Authentifikation. Es werden somit personengebundene und nicht nur personenbezogene Merkmale erfasst.

Biometrische Merkmale haben den Vorteil, dass sie nicht gestohlen und nur schwer kopiert werden können. Außerdem kann bei Passwort- oder Chipkartensystemen zwar überprüft werden, ob die Karte oder der Schlüssel gültig ist, es wird jedoch nicht überprüft, ob der aktuelle Benutzer auch der rechtmäßige Besitzer dieses Legitimationsmittels ist. Mit biometrischen Methoden kann dieses Sicherheitsmanko behoben werden.

Biometrische Verfahren können bezüglich Kosten und Leistungsfähigkeit eine Alternative zu anderen Sicherungsmechanismen darstellen oder diese ergänzen.

Unterscheidung Verifikation – Identifikation

Bei der ***Identifikation*** lautet die Fragestellung: Hier sind biometrische Merkmale, wer ist das? Dies bedingt eine Suche in einer zuvor angelegten Datenbank und ist eine typische Fragestellung der Polizei. Man nennt dieses Verfahren auch den ***One-to-many-Vergleich***.

Verifikation heißt der Vorgang, bei dem eine Person behauptet, XY zu sein, und dies dann mit einem biometrischen Vergleich zu beweisen hat. Dies ist eine typische Zutrittskontroll-Fragestellung, auch als ***One-to-one-Vergleich*** bezeichnet.

Einsatzgebiete Biometrischer Systeme

Systeme der persönlichen Authentifikation lassen sich überall dort einsetzen, wo sich Menschen gegenüber technischen Systemen identifizieren müssen.

In der SRG SSR idée suisse sind dies

- die Zugriffsbegrenzung und Kontrolle von zertifizierten Nutzern im Hinblick auf sensible Firmendaten (z. B. Lohn- und Gehaltslisten) oder vertrauliche Mitarbeiter- und Kundendaten.
- Beschränkung von EDV-Ressourcen (Anwendungen und Internet) auf einen festgelegten Benutzerkreis.
- Verbesserung der stationären Sicherheit durch absolut sicheren Zugang zu Gebäuden, Lagern und EDV-Räumen, Büros in öffentlichen Gebäuden, Labors und sendekritischen Systemen.

Nutzbare Eigenschaften zur Authentifizierung

Biometrische Identifikationsverfahren nutzen die Tatsache, dass verschiedene Körper- oder Verhaltensmerkmale einem bestimmtem Menschen eindeutig zugeordnet werden können. Mit Hilfe eines Sensors werden diese Merkmale bestimmt und dann einer Person eindeutig zugeordnet.

Messbare biometrische Eigenschaften einer Person gibt es viele. Einige davon finden sich in schriftlicher Form in jedem Pass. Sollen Messung und Vergleich mit vorher gespeicherten Daten jedoch automatisch erfolgen, so sind folgende Anforderungen an diese biometrischen Eigenschaften zu stellen:

- Invarianz der Eigenschaften: Diese dürfen sich über einen längeren Zeitabschnitt nicht verändern.
- Erfassbarkeit: Die Eigenschaften müssen in relativ kurzer Zeit messtechnisch erfassbar sein.
- Einzigartigkeit: Die Eigenschaften sollten genügend eindeutige Merkmale beinhalten, um die Person von jeder andern zu unterscheiden.
- Akzeptanz: Die Messung der Eigenschaften muss für ein breites Publikum in akzeptabler Form erfolgen. Auszuschliessen sind insbesondere invasive Techniken, d.h. Techniken, die zur Prüfung einen Teil des Körpers benötigen oder (scheinbar) beeinträchtigen.
- Reduzierbarkeit: Die erfassten Eigenschaften müssen auf einen leicht handhabbaren Datensatz reduziert werden.
- Zuverlässigkeit: Das Verfahren muss eine hohe Zuverlässigkeit und Reproduzierbarkeit aufweisen.
- Datenschutz: Die Privatsphäre der erfassten Personen ist zu schützen.

Unter diesen Voraussetzungen reduzieren sich die automatisch erfassbaren Eigenschaften auf wenige, welche alle in der Vergangenheit untersucht wor-

den sind. Die nachfolgende Tabelle gibt dazu eine Übersicht.

Eigenschaft	*Erfassung*	*Invarianz*	*Einzigartigkeit*	*Akzeptanz*
Handgeometrie	Optisch (IR)	gut	1:1000	sehr gut
Zwei-Fingergeometrie	Optisch (IR)	gut	1:1000	sehr gut
Augennetzhaut	Optisch (Laser)	sehr	1:1 Million	nicht gut (invasiv)
Augeniris	Optisch	sehr	1:6 Millionen	nicht gut
Venen Handoberfläche	Optisch (IR)	gut	unbekannt	sehr gut
Unterschrift	Dynamisch (Druck)	nicht gut	1:10000	sehr gut
Stimme	Elektroakustisch	nicht gut	1:10000	gut
Gesicht	Optisch oder IR	gut	unbekannt	gut
Fingerabdruck	Optisch, kapazitiv etc.	sehr gut	1:1 Million	gut

Tab. 1: Biometrische Eigenschaften

Andere Merkmale, wie zum Beispiel Gewicht, Grösse, Augenfarbe und Haarfarbe sowie besondere Merkmale fallen ausser Betracht, da sie Kriterien wie Einzigartigkeit, Möglichkeit messtechnischer Erfassung oder Invarianz nicht erfüllen.

Registrier- und Verifiziervorgang

Die technischen Voraussetzungen für die Verifizierung einer Person ist, dass die betreffende Person zuerst als XY im Erkennungssystem registriert und ein Datensatz abgespeichert wurde, der die biometrischen Merkmale festhält.

Jede biometrische Verifizierung beginnt deshalb mit der Registrierung. Dies soll gezeigt werden, am Beispiel der Fingerabdruck-Verfahren:

- Wahl einer PIN
- Präsentation des Fingers
- Berechnung des Fingermusters
- Weitere Präsentationen des Fingers
- Test

Nun soll verglichen werden, ob die als XY auftretende Person die selben biometrischen Merkmale aufweist. Dazu ist erforderlich:

1. Eingabe der behaupteten Identität der Person
2. Abruf des gespeicherten Datensatzes dieser Person aus einem Speicher
3. Messtechnische Erfassung der biometrischen Merkmale
4. Vergleich der erfassten Merkmale mit den gespeicherten Daten
5. Anzeige bzw. Verwertung des Resultats

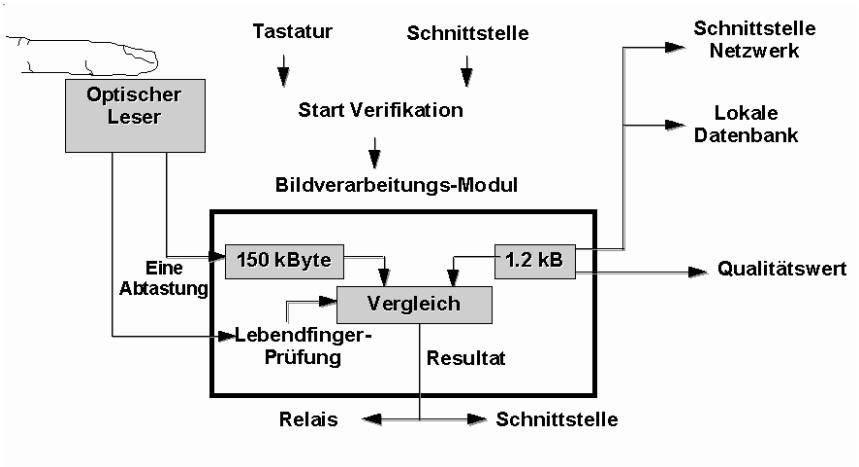


Abb.1: Prinzipieller Ablauf bei der Registrierung eines Fingerabdrucks

Biometrische Merkmale und ihre Erfassung

Der Fingerabdruck

Grundsätzlich erfolgt die Erfassung des Fingerabdrucks heute optisch: Der Finger wird auf ein Prisma gelegt; an den Berührungsstellen der Haut mit dem Prisma wird Licht gestreut (statt totalreflektiert), und das entstehende Bild wird mit einer CCD-Kamera aufgenommen.

Weitere Aufnahmeverfahren, wie Ultraschall-, Wärme/Druck- sowie kapazitive Verfahren sind getestet worden. Das Ultraschallverfahren ist wegen seines hohen Preises nicht eingesetzt worden. Das Wärme/Druck-Verfahren befindet sich noch im Versuchsstadium, während das kapazitive Verfahren heute schon eingesetzt wird.

Die anschliessende Bildverarbeitung und Verifikation kann auf grundsätzlich zwei Arten erfolgen.

Im einen Fall werden, wie die Polizei es tut, die sogenannten Minutien (endende Täler, Verzweigungen, Schweissporen) gesucht, vermessen

und das Resultat als Datensatz abgelegt. Bei der Verifikation werden die Minutien erneut vermessen und der neu entstehende Datensatz mit dem gespeicherten verglichen (minutiae matching, Minutienvergleich).

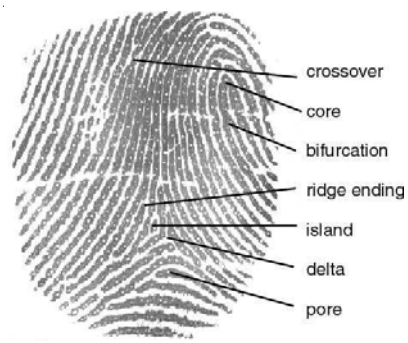


Abb. 2: Merkmale bei einem Fingerabdruck

Im zweiten Fall werden ausgesuchte Bildelemente als Datensatz gespeichert. Bei der Verifikation wird ausgehend von diesen Bildelementen nachgeprüft, ob auf dem präsentierten Finger diese Bildelemente vorhanden sind und mit dem Datensatz übereinstimmen (pattern matching, Mustervergleich).

In beiden Fällen werden ähnliche Sicherheitswerte erreicht; die Verifikationszeit kann jedoch im ersten Fall etwas länger sein.

Nur wenige Hersteller bieten eine sogenannte Lebendfinger-Erkennung an. Dabei geht es darum zu verhindern, dass eine Verifizierung mit einer Kopie (z.B. in Silikon) oder im Extremfall mit dem abgeschnittenen Finger einer registrierten Person erfolgen kann.

Bekannte Verfahren sind dabei die Erfassung der Farbe der Haut, ihrer elektrischen Eigenschaften und ihrer Reflexionseigenschaften.

Das Gesicht

Es existieren Verfahren zur visuellen und thermographischen Gesichtserkennung.
Die charakteristischen Merkmale der Gesichtszüge werden durch Auswertung eines Videobildes bestimmt.

Abb. 3: Gesichtserkennung

Mehrere dieser Verfahren sind erst in letzter Zeit bekannt geworden. Die Nähe zur Photographie lässt es für die Benutzer als sehr akzeptabel erscheinen. Zusammen mit den augenbasierenden Verfahren ist es völlig berührungsfrei.

Bezüglich Datenschutz sind einige Bedenken angebracht. So lässt sich das Verfahren für die Suche in einer Datenbank oder umgekehrt für die Suche bestimmter Personen in einer Menschenmenge einsetzen. Außerdem kann die Verifizierung unbemerkt vom Benutzer stattfinden, was bei den hand- und fingerbasierenden Systemen nicht möglich ist. Als Beispiel eines solchen datenschutzkritischen Einsatzes sei hier die Verwendung dieses Verfahren bei der Überwachung der Fussgängerzonen sowie der Fussballfans in den Stadien von England durch die Polizei erwähnt.

Die Iris (Regenbogenhaut) und die Retina (Netzhaut)

Die Netzhaut und die Regenbogenhaut gelten als sicherstes und unveränderlichstes Mittel, einen Menschen zu identifizieren, da sie sich auch bei eineiigen Zwillingen gut unterscheiden lassen. Eine Pupille wird entweder über einen „ungefährlichen“ Laser abgetastet oder per Video aufgezeichnet. Sind die Abgrenzungen und die charakteristischen Merkmale erfasst, werden sie wie ein „human-barcode“ abgespeichert.

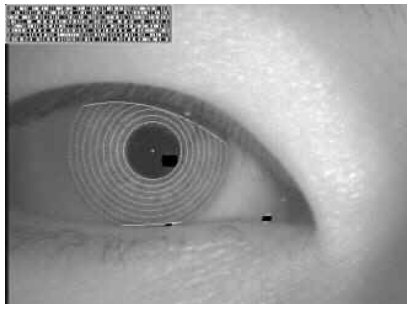


Abb. 5: Iris Scan

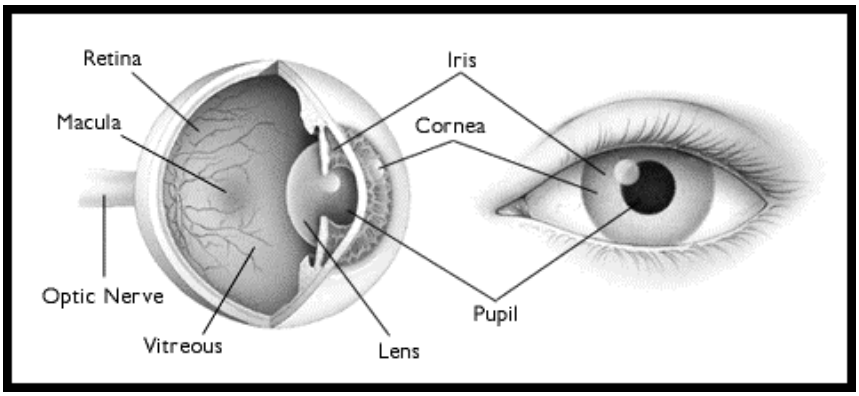


Abb. 4: Anatomie eines Auges

Schwierigkeit aller auf den Augen basierenden Verfahren ist einerseits die Hemmung der Benutzer, anderseits die Erfassung, das heißt die unterschiedliche Position der Augen relativ zum Gerät, das deshalb einen Suchvorgang durchführen muss. Es bestehen noch keine ausgedehnten Erfahrungen zu dieser Technologie.

Vergleich der biometrischen Systeme gegenüber konventionellen Verfahren

Vorteile

- Die Merkmale können im Unterschied zu karten- oder schlüsselbasierten Systemen weder verloren gehen noch an andere Personen weitergegeben werden.
- Die meisten der verwendeten Merkmale sind, über die für das System relevante Lebensdauer einer Person gesehen, verhältnismäßig unveränderlich (abhängig von der betrachteten Eigenschaft).
- Je nach Art des Merkmals ist die Fälschungssicherheit relativ hoch, Fälschungen sind in der Regel mit hohem Aufwand verbunden.
- Die Betriebskosten solcher Systeme sind geringer, da die Verwaltung von Karten beziehungsweise Schlüsseln und deren Ersatz bei einem Verlust entfällt.

Nachteile

- Biometrische Systeme sind in der Beschaffung teurer als konventionelle Systeme (der apparative Aufwand ist höher).
- Persönlichkeitsschutz kann eine Rolle spielen (je nach verwendetem biometrischem Merkmal und seiner Anwendung). Dies gilt insbesondere dann, wenn die biometrischen Merkmale neben der Verifikation auch zur Identifikation verwendet werden können.
- Hygienische Bedenken können ebenfalls eine Rolle spielen.

Kommerzielle Anwendung

Grundsätzlich sind die Anwendungsfälle für biometrische Systeme sehr zahlreich. Überall da, wo die Identität einer Person zweifelsfrei festgestellt werden soll, bieten sie klare Vorteile. Warum diese Art der Identifikation noch nicht weit verbreitet ist, hat wohl mehrere Gründe:

- Die Technik ist verhältnismässig neu. Erste im Handel erhältliche Geräte erschienen zwar bereits vor 15 Jahren auf dem Markt, waren aber unhandlich gross, langsam und exzessiv teuer.
- Die Umstellung bestehender Grosssysteme (z.B. der Verifikation des Bezügers an Geldausgabeautomaten) erfordert gewaltige Investitionen, so dass sich neue Systeme nur langsam durchsetzen.
- Der Preis für solche Geräte ist auch heute noch erheblich höher als zum Beispiel der Preis für einen Magnetkartenleser, obwohl die Preise tendenziell fallen.
- Sehr oft wird die mangelnde Akzeptanz bei den betroffenen Personen ins Feld geführt. Die Erfahrung zeigt jedoch, dass dieses Problem erheblich kleiner ist, als meist befürchtet wird.

Mangelnde Normierung veranlasste gerade Grossanwender, mit dem Einsatz noch zuzuwarten, da sie nicht einem einzelnen Lieferanten ausgeliefert sein wollen.

Zutrittskontrolle

Hier sind zahlreiche Anwendungen bekannt geworden, in der westlichen Welt allerdings meist in Ergänzung und nicht als voller Ersatz zu konventionellen Systemen.

Recht populär geworden sind in den letzten Jahren biometrische Systeme zur Sicherung von Kundenschließfächern in Banken, sowohl in Deutschland als auch in der Schweiz und zunehmend in Österreich. Hier gelangen sowohl Fingerabdruck- als auch Gesichtserkennungs-Systeme zum Einsatz.

Daneben sind in Banken, Gefängnissen, Kernkraftwerken, militärischen Anlagen, aber zunehmend auch in der Industrie und in weiteren Dienstleistungsbetrieben biometrische Zutrittskontrollen im Einsatz.

Ein möglicher Einsatz bei der SRG SSR idée suisse wäre eine zusätzliche Sicherung von Räumen, welche EDV- und sendekritische Systeme enthalten.

Sicherung von Computern und Datennetzen

In einschlägigen Kreisen ist allgemein bekannt, dass die Sicherung von Daten mit Passwörtern, wie sie heute meistens geschieht, äusserst problematisch ist.

Wenn sie nicht daran gehindert werden, verwendet die Grosszahl der Benutzer triviale Passwörter, wie den Vornamen, das Geburtsdatum und dergleichen.

Wird die Verwendung trivialer Kombinationen softwaremässig ausgeschlossen und ein regelmässiger Wechsel des Passwortes oder PIN zu häufig erzwungen, so beginnen die Benutzer die Passwörter aufzuschreiben, oft am Computer oder Terminal selbst oder dann zumindest in der obersten Schublade des Schreibtisches. Damit sinkt der Sicherheitswert beträchtlich.

In jüngster Zeit, und gefördert von den fallenden Preisen, sind jedoch vor allem Fingerabdruck-Systeme in Zusammenhang mit Datenschutz auf Com-

putern bekannt geworden. Hier eröffnet sich für biometrische Systeme ein Massenmarkt.

Drei Anwendungsfelder sind vor allem im Blickwinkel:
1. Zugangsschutz zum Computer selbst. In diesen Fällen wird entweder das Starten des Rechners oder aber der Zugang zum installierten Betriebssystem (z.B. bei Windows NT) oder der Zugang zu einzelnen Verzeichnissen auf der Festplatte gesichert.
2. Zugangsschutz zu Datenbanken und Programmen auf Servern, auf die über Clients zugegriffen wird. Der Schutz solcher Systeme bedarf zusätzlich des Schutzes der auf dem Verbindungsnetz übertragenen Information.
3. Elektronische Unterschrift. Wird die elektronische Kontrolle zum Beispiel von finanziellen Transaktionen auf Computernetzen gefordert, so bieten sich biometrische Systeme als besonders geeignet an. Ein Ziel ist hier auch die Sicherung bestimmter Vorgänge im hochgradig unsicheren Internet.

In der SRG SSR idée suisse kommt, zumindest heute, der Einsatz von biometrischen Systemen nur in den ersten beiden Anwendungsfeldern in Frage. Dies als Ergänzung zu den bestehenden Systemen.

Akzeptanz

Ein Kriterium zum Einsatz biometrischer Geräte ist die Frage nach der Akzeptanz durch die potentiellen Benutzer. So sind zum Beispiel hygienische Bedenken bei Systemen angebracht worden, die eine Berührung erfordern.

Allerdings berühren wir täglich Gegenstände, die vor uns andere Personen berührt haben (zum Beispiel Türklinken), so dass in der Regel die Berührung etwa eines Handgeometrie- oder Fingerabdrucksensors bedenkenlos erfolgt.

Die generelle Erfahrung zu diesem Problem ist, dass der Benutzer diese Art von Verifikation willkommen heißt, sofern er korrekt eingewiesen wurde, da sie einfach und sicher arbeitet.

Datenschutz

Die Hinterlegung biometrischer Eigenschaften einer Person tangiert deren Persönlichkeitsrechte und wird deshalb bezüglich Datenschutz relevant.

Dies gilt besonders für alle Fingerabdrucksysteme, deren Nähe zur polizeilichen Tätigkeit solche Fragen als naheliegend erscheinen lässt.

Nicht auf Fingerabdruck basierte Systeme sind zum Vorneherein weniger verdächtig, obwohl sich auch hier die gleiche Frage stellen lässt.

Nach Angaben von Spezialisten des Datenschutzes ist die Hinterlegung eines biometrischen Musters dann unbedenklich, wenn dies freiwillig geschieht und die diesen Dienst anbietende Organisation offenlegt, was sie mit der hinterlegten Information tut. Ausserdem sollte die Anwendung in einer Verifizierung vom Willen der betreffenden Person abhängen, also nicht unerkannt vorgenommen werden. Dieses Erfordernis erfüllen nicht alle Systeme in gleicher Weise. Gerade die berührungslosen Systeme (Augeniris, Gesichtserkennung) bieten hier Anlass zu Diskussionen.

Die Fingerabdruckmethoden stehen besonders im Schussfeld. Diese Methoden sind bezüglich Datenschutz unbedenklich, wenn das hinterlegte Muster die Rekonstruktion des Fingerabdruckbildes nicht zulässt. Ist dies gewährleistet, so sind die Muster für polizeiliche Suchzwecke wertlos und können nur in Kooperation mit der registrierten Person verwendet werden.

Völlig unbedenklich sind biometrische Systeme insbesondere dann, wenn das biometrische Muster nicht in einer Datenbank, sondern auf einer Karte gespeichert wird, die der Besitzer mit sich trägt (Kreditkarte zum Beispiel).

Etwas anders liegt die Situation bei Systemen, die in der Lage sind, Suchvorgänge in Datenbanken (one to many) durchzuführen. Hier gelangen wir an die Grenze dessen, was eine private Organisation durchführen darf. Diese Fragen sind jedoch von der örtlichen Gesetzgebung abhängig: Die Vereinigten Staaten lassen diesbezüglich viel mehr Freiheit für private Organisationen zu als die europäischen Länder.

Marktaussichten

Gemäss den Angaben der Gartner Group und der International Biometric Industry Association (IBIA) ist eine rasante Aufwärtsentwicklung der biometrischen Systeme zu erwarten.

Mit der Verfügbarkeit immer billigerer, kleinerer und einfach zu handhabender Systeme werden diese Technologien besitz- und wissensbasierte Systeme (Passwörter, Badges usw.) in sehr vielen Bereichen sicher nicht vollständig ablösen, aber teilweise ersetzen oder mindestens ergänzen.

Genau so wie sich der Benutzer an Magnetkarten, Chipkarten und an Passwörter gewöhnt hat, wird er sich an die biometrische Verifikation gewöhnen. Bequemlichkeit und Sicherheit dieser Systeme dürften schliesslich auch die Skeptiker davon überzeugen, dass es sich um natürliche Verfahren der automatisierten Erkennung von Personen handelt.

Die Erfassung biometrischer Eigenschaften ist technisch nicht unproblematisch. Das bedeutet, dass sie mit einem apparativ hohen Aufwand verbunden ist, um zuverlässig zu arbeiten. Dies ist aber kein grundsätzliches Hindernis für die Verbreitung dieser Technologie, da Preiszerfall der Elektronik und Miniaturisierung weiter fortschreiten und damit immer weitere Anwendungsbereiche ermöglichen werden.

Markus Gander, SRG SSR idée suisse Bern

Biometrie

Biometric ID Card Debates

Malaysia, Hong Kong, Brunei and Macao are all examples of countries where electronic identity cards that use biometric data such as your fingerprint, iris patterns or facial characteristics are already in everyday use. Many other countries are still debating whether or not biometric ID cards should be introduced. In order to realise the advantages biometric technologies can offer, several important issues need to be properly addressed.

What are biometric identity cards?

There are three basic elements of identity:

- Biometric identity consists of attributes that are unique to an individual, including iris patterns, fingerprints, voice, retinal patterns, facial structure, DNA profile, hand geometry etc;
- Attributed identity consists of the components of a person's identity that are given at birth, including their full name, date and place of birth, parents' names and addresses;
- Biographical identity, which builds up over time, includes employment records, address history, details of benefits claimed/taxes paid, registration of marriage etc.

Unlike traditional identity documents such as birth certificates, passports or driver's licences, new national identity schemes call for a mixture of biometric, attributed and biographical data to be stored electronically on a smart card and/or in a central database. The basic idea is that new technologies enable authorities to compare a biometric reading taken from an individual against the stored template. Since biometrics are unique to individuals, only authorised individuals will be granted access to social benefits and services.

Versatility

The electronic ID cards of the future will be suitable for a variety of applications. A biometrically enabled multi-application card could securely integrate an identity card, a driver's licence, an eGovernment card with a digital signature for filing tax returns or online voting, a payment card, a health card, commuter passes for public transportation systems etc.

Arguments in favour of biometric IDs

Identity fraud

The last large-scale identity theft research performed in the UK (Cabinet Office, 2002) suggests that the minimum quantifiable cost to the British economy arising from identity fraud is at least GBP 1.3 billion per annum. However, the report warns that even for 2002, this figure is certainly an underestimate, as it does not include areas such as Local Government, health services or education where it is known that identity fraud exists but there was not sufficient data available to estimate the cost. Additionally, identity theft is one of the fastest growing crimes: A current estimate suggests that a person's identity is

stolen every 4 minutes on average in the UK.

If a central record of biometrics is kept, authorities can ensure that every individual can only be enrolled into the system once. This would lead to a near-elimination of multiple identities and therefore to a considerable cut-down on costs associated with identity fraud as social benefits could only be claimed once.

Terrorism and organised crime

Furthermore, if biometric identification was required for opening and accessing bank accounts, possibilities to launder money would be more limited than it is today. In turn, organised crime units and sleeping terrorist cells would find it harder to operate, thus enhancing national security.

Illegal immigration

As an additional advantage, a national biometric identification scheme would also help to control illegal immigration through limiting access to services and resources that are considered essential for living, e.g. health services, property rental, bank transactions, driver licensing etc.

User benefits

Legitimate users of the scheme would therefore benefit from living in an overall more secure environment. Additionally, the introduction of a multi-purpose card would also enhance user convenience as it has the potential of combining several card functions into one.

Voices of the opposition

Privacy

The use of biometrics involves a certain loss of autonomy and anonymity, since users of such systems are exposing information about themselves in the form of a biometric identifier. This data could be used to establish identity over large-scale databases, possibly even without the user's knowledge. Some technologies (e.g. face recognition) also allow the tracking of users.

However, biometric data does not constitute information that could be regarded as secret or private: our facial images are recorded every time we enter a bank, supermarket or even just pay at the petrol station; our voices are recorded by many phone-based service providers; and we leave our fingerprints and DNA behind everywhere we go. Furthermore, the tracking of individuals is already possible using alternative - and widely accepted - technologies: How many people use mobile phones, GPS satellite navigation or credit cards on a daily basis?

„Function creep"

Once a biometric identifier is captured, the generated template can easily be copied and shared among different databases, enabling the build-up of extensive user profiles, even without the user's knowledge or consent. Such user profiles could potentially contain police and tax records, travel activities and more.

It is important to understand that the possibility of linking databases in order to create extensive profiles of individuals has nothing to do with biometrics in general. Databases containing sensitive information do already exist and they also could easily be joined using common identifiers as keys, such as taxpayer identification numbers, ID, passport, driver's license and other registration sequence numbers. Therefore, controlling the use of biometrics does not provide any protection against this threat. The only solution to this problem is through corresponding legislation that regulates the use of contemporary information systems.

Stolen biometrics

Another concern that arises in connection with central storage of biometric data is that a single database is a very attractive target for hackers. As a result, we must think about the possible consequences of biometric credentials being stolen from a national or even international database. At the same time, we must accept the fact that biometric information cannot be regarded as secrets as explained above.

Therefore, the real threat is not that someone could get hold of our biometric information because this is possible through far simpler means than hacking a database. Instead, methods must be put in place to ensure that biometric samples submitted were not generated by some fake artefact. Technologies do exist that make reliable liveness testing a reality. However, decision makers must be aware of spoofing-related threats in order to opt for the deployment of appropriate countermeasures.

Accessibility

A small fraction of the population will not be able to enrol their fingerprints or iris images. This is due to the fact that these features are not fully universal, i.e. not everyone has fingers or eyes that can be used for recognition purposes, in addition to those who do not have fingers or eyes at all. Physical workers often have fingerprints that

are so worn and/or affected by chemicals that they are unreadable by most sensors. Furthermore, people suffering from aniridia cannot be identified by their irises. Aniridia is a rare medical condition (occurs in one in 75,000 persons) in which a person lacks one or both irises. Additionally, people with nystagmus (tremor of the eyes) might have problems presenting a stable image; however, there are iris cameras that use flashed infrared illumination with very fast integration times, so that tremor becomes unimportant for image capture.

In short, when a national-scale biometric system is discussed, it must be taken into consideration that a certain fraction of the population will not be able to use it or at least will need special assistance and/or hardware in order to seamlessly interact with the technology. Furthermore, sufficiently secure bypass methods need to be accessible for those that are unable to present any of the biometric features in use. It is also important that these people do not feel discriminated because of their disabilities.

Identity management

Obtaining a biometric ID card still depends on the presentation of traditional documents such as birth certificates and driver's licences. Recording a mixture of biometric, attributed and biographical data ensures the reliable binding of a person to a set of data. However, it is still possible that the cardholder presented fake documents when the card was issued.

This is a serious issue that needs to be addressed in at least the following two ways. Firstly, it must be ensured that individuals cannot enrol into the system more than once. The only way to do that is to establish a central register that contains biometric data that is sufficiently unique to allow exhaustive searches in a large database. Secondly, audit trails need to be defined, maintained and accordingly controlled across all organisations that are involved in the registration and administration of data.

Costs

When the UK Identity Card Bill was published in November 2004, the government estimated that the costs of the scheme over ten years would be GBP 5.5 billion, almost twice as high as the original estimate made in 2002 in the order of GBP 3.1 billion. Although the costs of identity fraud over ten years easily outweigh even the higher figure, industry specialists have warned that unexpected problems could create higher costs.

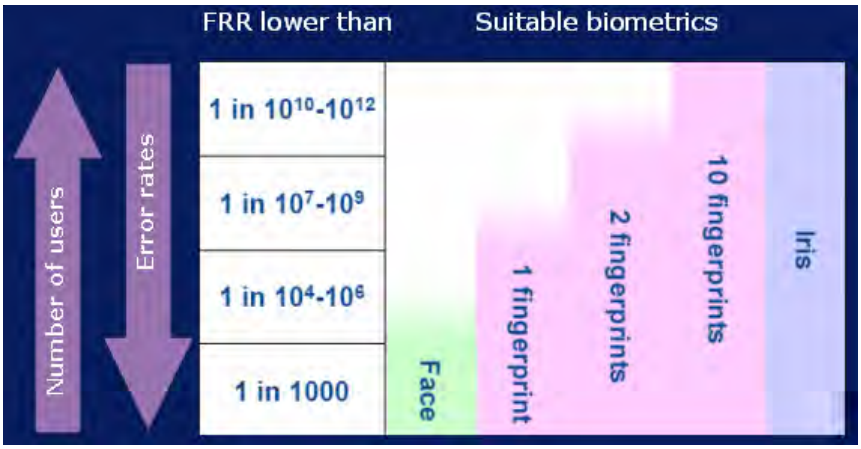
Health implications

Iris recognition often raises the concerns whether long-term use of the technology could potentially be damaging to the eye and whether iris images could be used for health diagnostics. While both concerns are scientifically unfounded, they must be addressed in order to enhance public acceptance of the technology. Furthermore, sensors that require physical contact (e.g. almost all fingerprint recognition devices) often raise hygiene concerns and not without reason. Any surface that is frequently touched by large masses of individuals collects residuals that not only raise hygiene concerns but can also affect system performance. Therefore, appropriate cleaning solutions need to be adopted if contact sensors came into large-scale public use.

Further issues to be considered

Technology selection

The most important technical factor that needs to be looked at especially for large-scale implementations is the operational error rates. The more people use the system, the lower the error rates must be in order to ensure seamless processing. As presented in the figure below, which is based on Dr Tony Mansfield's findings at the National Physical Laboratory in the UK, iris recognition is to be considered more accurate than even the scanning of 10 fingerprints. Nevertheless, each proposed biometric – face, finger and iris – has its own advantages and limitations, as described below.



Comparison of proposed technologies (based on Mansfield, 2004): the more people use the system, the lower the false rejection rate (FRR; percentage of enrolled people not being recognised by the system) must be. Iris recognition is considered to be more accurate than the scanning of even 10 fingerprints.

Fingerprinting is the oldest technology, relatively inexpensive to deploy and we have extensive fingerprint databases of criminals to compare against. However, the uniqueness of fingerprints is limited and many users would require special hardware in order to enrol and recognise hardly visible fingerprints. Additionally, not everyone has fingers and most hardware platforms are very easy to spoof.

Experts generally agree that iris recognition is by far the fastest and most accurate biometric technology available. Iris recognition is the only technology that has an established false acceptance rate (percentage of identity mismatches) of zero. Additionally, methods exist that make the technology highly resistant to spoofing. However, image acquisition can be difficult in certain cases and irises are not fully universal, as already mentioned above.

Finally, face recognition has the advantage that everyone has a face, we again have extensive facial image databases of criminals and the technology can be active without the users' knowledge (while this is an advantage from a technical point of view, privacy experts regard this as a disadvantage). At the same time, the uniqueness of faces is very limited which often results in unacceptably high error rates. Additionally, unlike irises and fingerprints, faces change considerably over time, which would require frequent re-enrolment of facial images.

Hardware selection

Once decision makers agree on the technologies to be used, the next challenge will be the selection of the appropriate hardware. Firstly, hardware platforms differ greatly in terms of throughput rates, user convenience, resistance to spoofing etc. Secondly, an open architecture should be adopted so that hardware can be upgraded modularly as soon as more advanced devices appear.

Data storage

It has already been mentioned above that central storage of biometric data is essential in order to screen out multiple identities. If biometrics would only be stored on smartcards, governments would lose the ability to meet their most important target: To cut down on identity fraud. Nevertheless, storing the biometric templates on smart cards, in addition to a central register, would offer further advantages, including the option for local, one-to-one matching of the presented biometric to the template on the card without any need to connect to a central database.

Mandatory vs voluntary cards

Undoubtedly, most benefits could only be realised if biometric ID cards were mandatory; however, we need to be aware of the implications of this. Firstly, several nations currently discussing the rollout of biometric IDs are not used to the idea of having to carry a card for identification purposes; some nations, such as the British or the Danish, are not even used to the idea of having an ID card at all. Secondly, mandatory enrolment would mean that everyone has to pay for the new card and that everyone has to appear in dedicated centres in order to have their biometric measurements taken and documents checked. This might pose difficulties especially for those living outside major conurbations. Thirdly, even if a voluntary scheme was introduced, not having an ID card might be interpreted as suspicious behariour which would create an indirect pressure on citizens to apply and pay for a card.

Conclusion

Many issues need to be tackled and it must be kept in mind that biometrics are not a panacea. Nevertheless, a wisely designed biometric identity card scheme could offer a wide range of benefits to governments and citizens alike. As described above, most arguments that are frequently used in debates against biometric identity cards actually do not oppose the idea; they only call for expert evaluation and consideration of important matters.

Even in the UK, where public opinion has typically seen identity cards as an infringement of civil liberties, there was a major shift in public opinion: A Mori poll of 1,000 people, conducted in April 2004, indicated that 80% backed a national ID card scheme. Furthermore, a recent report of the Joint Research Centre of the European Commission concludes that initial public sector use of biometrics will create further confidence and therefore, give way to a wider use of these techniques in commercial and civil applications.

For more information about this topic or the fully vendor-independent biometric consulting and security auditing services Deloitte offers worldwide, please visit our website at www.deloitte.co.uk/biometrics or contact me at boritoth@deloitte.co.uk or +44 7840 389 909.

Bori Toth, Biometric Research and Advisory Project Lead, Deloitte & Touche LLP, London

Biometrie

Die Zukunft gehört der Biometrie

Das Marktsegment Zutrittskontrolle und Zeitwirtschaft ist nach wie vor stark in Bewegung. Auf der Identifikationsseite setzten sich berührungsfreie Konzepte nachhaltig durch und erreichen heute 90% der neu installierten Anlagen. Mechanische Schliessanlagen, elektronische Zutrittskontrolle und Zeiterfassung sowie Sicherheits- und Automatiktüren wachsen zu einem Leistungsprogramm „rund um die Tür“ zusammen und werden perfekt aufeinander abgestimmt. Mit der Verbilligung und entsprechenden Verbreitung von Netzwerken entsteht das Bedürfnis, alle Datensysteme miteinander zu vernetzen; drahtlose und virtuelle Netzwerke verstärken diesen Trend.

Auf der juristischen Seite wächst der Anspruch auf die Revisionsfähigkeit von Vergaberechten für den kontrollierten Zutritt zu physischen und logischen Datenräumen. Im gleichen Atemzug muss auch das damit zusammenhängende ungelöste Haftungsproblem beleuchtet werden. Wer haftet für einen unerlaubten Zugriff im Datenschutzraum? Auch wenn alle Massnahmen, wie eine Begrenzung der Anzahl Zutrittsberechtigter, eine Personenvereinzelung und ein IT-gestützter Workflow für einen lückenlosen Nachvollzug der Berechtigungsvergabe getroffen sind, fehlt die eindeutige Identifikation der zutrittsberechtigten Person. Das gelingt nur über die biometrische Identifikation oder Verifikation.

Die Auswahl an biometrischen Systemen ist sehr vielfältig, weil der Mensch in verschiedenen Körperbereichen einmalige Erkennungsmerkmale besitzt. Das ultimative biometrische Erkennungsmerkmal wäre wohl die DNA-Analyse. In der Praxis haben sich aber einfachere und billigere Verfahren durchgesetzt. Das verbreitetste ist wohl der elektronische Fingerabdruck. Aber auch das Gesicht und die Retina wurden schon frühzeitig als Erkennungsmerkmal ausgewertet. Heute im Markt erhältliche Systeme können in folgende Kategorien eingeteilt werden:

- Fingerprint, d.h. Auswertung des Fingerreliefs
- Glieder- und Venengeometrie der Hand
- Retinavermessung
- Gesichtserkennung (optische Merkmalauswertung im sichtbaren oder Infrarot-Bereich)
- Stimmerkennung etc.

Ein einziges Erkennungsmerkmal deckt nicht alle Anwendungsbedürfnisse ab. Zum Beispiel scheiden in einem Bereich mit Handschuhpflicht Hand und Finger als biometrisches Merkmal aus, wo Gesichtsmasken getragen werden, ist die Gesichtserkennung nicht anwendbar, Stimmerkennung scheidet in lärmintensiver Umgebung aus, usw.

Verfahrenstechnisch wird grundsätzlich zwischen der direkten biometrischen Erkennung und der biometrischen Verifikation eines Berechtigungsmittels (zum Beispiel Pass oder Personalausweis) unterschieden.

Bei der direkten biometrischen Identifikation werden biometrische Referenzdaten in einer Datenbank mit den Messdaten an einer Person verglichen. Die biometrische Verifikation vergleicht die Messdaten mit der auf einem Berechtigungsmittel gespeicherten Referenz. Die Verifikationsmethode hat den Vorteil, dass das Messergebnis 1:1 mit der Referenz auf Übereinstimmung geprüft werden kann, während bei der direkten Identifikation das Messergebnis mit einer Vielzahl von Referenzdaten aus einer Datenbank verglichen werden muss. Nachteilig ist bei dieser Methode der relativ lange Suchprozess, die Abhängigkeit der Reaktionszeit von der Anzahl Berechtigter und die weitaus geringere Trennschärfe.

Vor allem aber besteht ein nicht unerhebliches Sicherheitsrisiko beim Zugriff auf die in der Datenbank hinterlegten (einmaligen) Referenzdaten. Die Referenzmethode umgeht dieses Problem durch die eigenverantwortliche Verwahrung der kritischen Referenzdaten auf dem persönlichen RFID[1]-Ausweis oder Schlüssel. Bemängelt wird bei dieser Methode oft die Notwendigkeit eines physischen Berechtigungsmittels, was im betrieblichen Umfeld allerdings kaum zum Tragen kommt, weil häufig ohnehin ein Personalausweis oder Schlüssel zum Einsatz gelangt. Wird dieser in moderner RFID[1]-Technologie (z.B. Legic® [2]) ausgeführt, dient er gleichzeitig als Datenträger der biometrischen Referenzdaten und kann zusätzlich für alle nicht-biometrischen Berechtigungen, wie Zutritt, Zeitwirtschaft und Datenerfassung, so wie als bargeldloser Wertträger für Kaffeemaschinen, im Personalrestaurant und für die Parkgarage eingesetzt werden.

Im Heim-Anwendungsbereich kommen die Nachteile der identifizierenden Methode weniger zum Tragen, weil die Datenmenge an Referenzdaten klein ist und der Zugriff darauf im persönlichen Verantwortungsbereich liegt.

Das Akzeptanzproblem von biometrischen Anwendungen ist auch mit modernen, kostengünstigen und komfortablen Lösungen nicht ganz ausge-

räumt. Viele Benutzer haben hygienische Bedenken, wenn sie Hand oder Finger auflegen müssen, obwohl sie ohne zu studieren jeden Tag wiederholt Türklinken, Lichtschalter und Tastaturen betätigen. Hinzu kommt, dass es noch keine kommerziell verwendbare biometrische Abstandserkennung von sich bewegenden Personen gibt. Aber daran wird in namhaften Instituten in verschiedenen Teilen der Welt intensiv gearbeitet.

Zukünftige Systeme basieren auf der dynamischen Gesichtserkennung. Das heisst, dass das Gesicht während des Zugehens auf eine Tür automatisch erfasst und mit der auf Distanz erfassten Referenzdatei in der Chipkarte verglichen wird. An der Tür angelangt, ist der ganze Identifikationsprozess abgeschlossen, ohne das aktive Zutun der zu identifizierenden Person. Diese sogenannte „Pförtnerlösung" erreicht die maximale Akzeptanz, zumal sich jedermann gewohnt ist, am Gesicht identifiziert zu werden.

Auch wenn solche Verfahren noch einige Jahre Entwicklungszeit bis zum praktischen Einsatz benötigen, bieten moderne Biometriesysteme, wie z.B. das Kaba® biover[2] kein technisches oder kommerzielles Hindernis mehr, die Vorteile der biometrischen Identifikation in einem erweiterten Anwendungsbereich zu nutzen.

Ulrich P. Wydler, Direktor der Kaba Holding AG, Rümlang (Schweiz)

Endnoten

1 RFID Radio Frequency IDentification (berührungsfreie Identifikation)

2 Legic® und Kaba® biover sind geschützte Marken der Kaba Holding AG, Rümlang (Schweiz)

Biometrie

Sind biometrische Systeme teuer, aber sicher?

Das IT Governance Institute hat sich im Jahre 2004 zu diesem Thema mit einem lesenswerten Papier geäussert (ISBN 1-893209-55-5). Ich fasse daraus die mir wichtig erscheinenden Erkenntnisse zusammen.

Grundsätzliches

Zuerst ist zwischen Bestätigung (Verification) und Erkennung (Identification) zu unterscheiden. Im ersten Fall geht es darum, einem bekannten Individuum Zutritt bzw. Zugriff zu gewähren. Im zweiten Fall geht es darum, herauszufinden, wer die sich präsentierende Person überhaupt ist.

So gesehen dürfte die Verification als die „einfachere" Anwendung der Biometrie bezeichnet werden dürfen, wird doch im Normalfall nur einer beschränkten Anzahl Personen der Zutritt zu einem Raum gestattet, d.h. es wird auch nur eine beschränkte Anzahl von Merkmalen im System gespeichert werden, weil „alle anderen" als ungültig abgewiesen werden müssen. Im zweiten Fall ist dagegen die Anzahl zu speichernder Informationen gegen oben theoretisch nicht limitiert, indem in der Datensammlung gesucht werden muss, ob Merkmale der zu prüfenden Person zutreffen.

Aus Sicht des Datenschutzes ist die Verification wohl weniger problematisch, weil die betroffenen Personen ein Interesse daran haben müssen, als „Berechtigte" erkannt zu werden. Bei der Identification dagegen könnten Persönlichkeitsrechte verletzt werden, wenn es z.B. darum geht, den Aufenthaltsort einer bestimmten Person zu einem bestimmten Zeitpunkt zu bestimmen.

Somit ist bei allen zur Anwendung gelangenden Techniken immer zu hinterfragen, welche Absicht hinter der Anwendung der Methode steht.

Fingerabdruck

Nicht erst seit Connon Doyle und Sherlock Holmes ist dies die klassische Methode der Biometrie. Sie wurde übrigens als Markenzeichen bereits vor Jahrtausenden von asiatischen Töpfern verwendet. Die Verbreitung der Anwendung ist heute erheblich und im Erkennungsdienst bei der Polizei „tägliches Brot".

Die Kosten für Scanners von Fingerabdrucken sind in letzter Zeit beträchtlich gesunken und sind für CHF 100 bis 300 zu haben. Für Leser muss mit bis zu CHF 40 000 gerechnet werden; das Zutrittssystem kostet gegen CHF 5000, und die Lizenzen für eine solche Software liegen bei CHF 5 pro betroffene Person.

Da die Methode in erster Linie als Polizei-Instrument bekannt ist, erfreut es sich nicht unbedingt grosser Beliebtheit, was die Verwendbarkeit teilweise einschränkt. Ebenso ist das System für Leute ohne Finger(beeren) oder solche, die einen harten handwerklichen Beruf ausüben (Verletzungen, Abrieb) nicht geeignet. Die Fehlerrate (d.h. zwei Individuen haben den gleichen Fingerabdruck) liegt bei über eins zu einer Milliarde und gilt deshalb als gesichert.

Handgeometrie

Sie basiert auf der Erkenntnis, dass sich die Handstruktur grundsätzlich ab dem 13. Altersjahr nicht mehr ändert.

Die Akzeptanz der Technik ist gemäss Untersuchungen gross. Die Kosten bewegen sich zwischen CHF 2500 und 6000.

Bezüglich Sicherheit schneidet diese Methode etliches schlechter ab als der Fingerabdruck, weil die Handstruktur nicht als „einzigartig“ bezeichnet werden kann. Zudem ist die Methode bei Personen mit erheblichen Handverletzungen oder gar Amputationen nicht anwendbar.

Netzhaut-Scanning

Die Struktur der Blutbahnen und Nervennetze bleiben über die Lebenszeit einer Person praktisch konstant und gelten als einzigartig, was sogar bei eineiigen Zwillingen bereits in den Fünfzigerjahren des vergangenen Jahrhunderts nachgewiesen werden konnte.

Die relativ hohen Kosten schrecken viele potentielle Anwender ab. Die fest zu installierenden Geräte kosten über CHF 3000 und tragen den Nachteil, dass der Unterhalt der Geräte sowie die Anwendungsbetreuung teuer sind. Die betroffenen Personen müssen sich sehr nahe an die Geräte begeben und sich während der „Aufnahme“ nicht bewegen, was für die Akzeptanz nicht gerade förderlich ist.

Viele Personen betrachten das „Ausschnüffeln“ ihrer Augen als voyeuristisch und befürchten auch zufällige Augenverletzungen. Die Sicherheit kann als sehr hoch eingestuft worden, wobei allerdings eine Gruppe mit Leuten mit gewissen Augenleiden oder -verletzungen für diese Methode nicht geeignet ist.

Regenbogenhaut-Scanning

Die Technologie beruht auf der Erkenntnis, dass die Struktur der Regenbogenhaut vielerorts ebenfalls als praktisch einzigartig pro Individuum betrachtet werden darf. Die Methode hat gegenüber dem Netzhaut-Scanning den Vorteil, dass die erkennenden Instrumente weiter entfernt sein können und somit das Gefühl der „Persönlichkeitsverletzung durch Eindringen“ weniger zum Tragen kommt.

Die Kosten sind allerdings noch beträchtlich (ca. CHF 7000 Lizienzgebühren und gegen CHF 600 pro Gerät).

Die anfänglich vermutete Einzigartigkeit der Regenbogenhaut muss relativiert werden, indem kürzlich eine Sicherheitsrate von lediglich 95% festgestellt wurde. Zudem ist eine gewisse Bereitschaft zur Zusammenarbeit mit der zu prüfenden Person notwendig, auch wenn nicht im gleichen Ausmass wie beim Netzhaut-Scannning.

Gesichtserkennung

Wer kennt sein Passbild nicht?! Der Ausspruch, dass man gar nicht so alt werden kann, wie man darauf aussieht, ist für „Freunde“ ein geflügeltes Wort. Dennoch ist dies wohl die am weitesten verbreitete Methode der Biometrie. Allerdings bedurfte sie bis vor wenigen Jahren des Erkennungsgerätes Mensch, was sie für Viele wegen der angeborenen Subjektivität der Menschen disqualifizierte. Neuerdings hat aber auch hier die Technologie zugeschlagen und die Gesichtsmerkmale festgehalten und digitalisiert.

Ein voll integriertes System ist enorm teuer (bis zu CHF 300 000) und hat einen schlechten Sicherheitsfaktor. Demnach können es sich nur grosse Institutionen (wie Interpol) leisten. Die Sicherheitsquote ist übrigens schlecht, weil durch künstliche Gesichtschirurgie, Unfälle, Naturlaunen wie eineiige Zwillinge und Alterung der Grad der Sicherheitsbestimmung abnimmt.

Unterschriftsdynamik

Mit der Mechanisierung des Leistens von Unterschriften (anstelle von Stempeln) wurde erkannt, dass nicht nur der (graphische) Schriftzug an sich, sondern auch der sich während der Unterschrift verändernde Druck auf das Schreibgerät eine Rolle spielen. Graphologen hatten schon viel früher erkannt, dass nicht nur die graphische Gestaltung der Schrift, sondern noch andere Elemente bei der Analyse der Schrift eine Rolle spielen.

Diese Technik gehört mit etwa CHF 20 per Betroffenem zu den heute billigsten auf dem Markt, wobei die Unsicherheitsmarge relativ hoch ist. Erstaunlich, dass viele Rechtssysteme aber auch heute noch auf einen hohen Stellenwert auf „eigenhändige“ Unterschriften legen. Vielleicht liegt es paradoxerweise gerade an dieser Unsicherheit, dass die Akzeptanz des Systems erstaunlich hoch ist. Es ist sicher jedermann aufgefallen, dass sich die Unterschrift im Verlauf der Zeit verändert. Wenn Sie daran zweifeln, sehen Sie einmal ein von Ihnen unterzeichnetes Schriftstück an, dass Sie vor über zehn oder gar zwanzig Jahren erstellten!

Tastaturdynamik

„Der haut in die Tasten.“ Wie jeder Pianist seine eigene Anschlagstechnik hat (es bestehen seit Lochkartenzeiten Partituren, welche die Aufführung berühmter Pianisten aufleben lassen, bei denen auch der Anschlag „original“ ist – wie in Musikmuseen in Erfahrung gebracht werden kann), so

schlägt jede Person individuell die Schreibmaschinentastatur an.

Die Kosten für diese Geräte belaufen sich auf CHF 50 bis 150 pro betroffener Person.

Die Angst vor „spoofing“ und Imitation fremder Personen hindert daran, dass eine weitere Ausbreitung der Erkennungsmethode zur Anwendung gelangt. Zudem ist die Rate der „unbekannten Tipper“ relativ hoch. Dies mag an der Tagesform der betroffenen Personen hängen, an Verletzungen, Rheumaerkrankungen oder schlicht der Änderung von Gewohnheiten.

Stimmenerkennung

Der Foxterrier, der auf der Schallplatte auf ***His Masters Voice*** hört, illustriert den Advent der Voice recognition. Sie basiert auf dem Anspruch, dass jeder Mensch über eine ihm eigene Stimme verfügt, deren Merkmale sich digitalisieren und vergleichen lassen. Künstler, deren kabarettistischen Imitationen das Publikum zu Lachstürmen provozieren, lassen an diesem Anspruch allerdings zweifeln.

Die Geräte sind relativ teuer (CHF 5000 bis 10 000), so dass sich die Technik wohl eher auf die Umsetzung von Informationen in das geschriebene Wort konzentrieren wird. Zudem beeinträchtigen bereits harmlose Erkrankungen (Schnupfen, Heiserkeit) die Sicherheit der positiven Erkennung in erheblichem Masse.

Fazit

Von den drei Erkennungsmerkmalen: Was jemand hat, was jemand weiss und was jemand ist, ist das letztere Merkmal wohl das sicherste. Die verschiedenen Methoden und Techniken auf diesem Gebiet sind heute weit gediehen, doch keines kann für sich in Anspruch nehmen, absolut sicher und universell anwendbar zu sein. Ihr Preis ist nach wie vor hoch, auch wenn Tendenzen zur Verbilligung zu erkennen sind. Am sichersten ist wohl nach wie vor eine Kombination der drei genannten Elemente.

Max F. Bretscher

Corporate Governance

How the culture of an organisation affects Governance

The seminar at this year's Annual Meeting of the ISACA Switzerland Chapter was given by Mr. Ivan Moss (Partnerships Program Manager, IMD, International Institute for Management Development, www.imd.ch.) Using a case study he explored the links between Company Culture and Governance.

Corporate Governance tends to flash Enron and Parmalat signs in people's minds. Often the perception is that bad Governance is linked to dubious dealings, which are relatively distant from the daily running of IT Departments. This context made the selection of TXUE as the case study an intriguing choice.

The analysis of the workings of TXUE, a UK Electricity company, prior to its demise was not the expected story of illegal activities. At first sight, the failure of the company appeared to be due to bad luck following an understandable taking of business risk in a changing market place.

However, was there another reason why this healthy company was the only example among several other UK Electricity Companies, which lost performance and went bankrupt? Further analysis uncovered a grave problem of governance.

The ultimate goals of corporate governance are, it can be argued, to:

- safeguard the profitability of the company (to protect the investments of shareholders, the jobs of employees), and
- fulfill the company's wider social responsibilities – at a minimum, compliance legal and regulatory requirements such as environmental, health and safety standards.

Further analysis and discussion provided a deeper analysis of some of the real causes of failures in corporate governance.

TXUE had fulfilled all of the modern regulatory requirements and best practices for corporate governance. But despite the existence of extensive management processes and procedures, TXUE failed. Why?

By looking at Galbraith's Star Model for organizational design, we were able to see more clearly the underlying causes of TXUE's decline and so its failure in its duty of corporate governance.

The Esssentials

The case study constitutes a warning of the consequences for an organization if the essential considerations are neglected.

Behavior affects ***Culture*** and ***Performance***

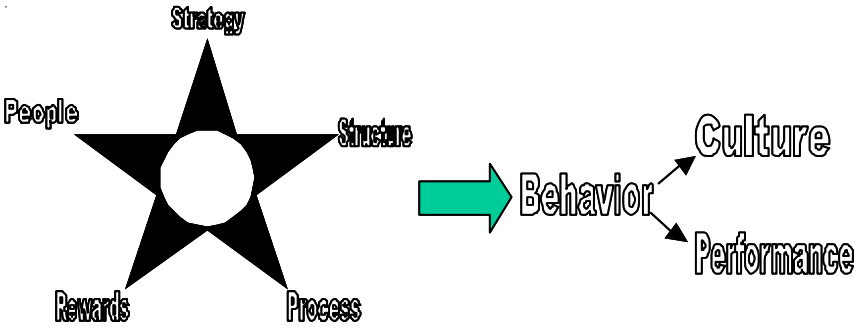
Behavior is affected by:
Strategy – Strucuture – Process – Rewards – People

It can be argued that TXUE had a poor strategy (misjudging the long-term changes in the industry), weaknesses in its organizational structure (particularly between the UK subsidiary and its US parent company), gaps in its information and decision processes (particularly in responding to changing regulations and market conditions) and rewards and incentives programs which were not aligned.

As such, it is possible that the weaknesses in TXUE's organizational design are such that problems in corporate behavior and performance were not adequately recognized and challenged until too late.

In analyzing the case of TXUE, Ivan showed us how TXUE had, over a number of years, taken a series of key decisions, which together moved the company's strategic position and changed its risk profile – both in terms of the level of risk and the types of risk TXUE managed in its business. In addition, a number of those decisions were unsuccessful, and so it can be argued that the event, which finally 'killed' TXUE was not one simple moment of bad luck.

Is this warning story relevant to IT Governance?
Ivan asked: „Could something like this happen in an IT organization? In your organisation?"



The discussion was lively and thought provoking. The response of the audience was an unequivocal „Yes“. The same issues present in Galbraith's Star Model exist in IT departments and in the relationships of IT Departments with other Business departments. Indeed, several participants felt that these issues are more pertinent than ever, because it is increasingly difficult to balance the short-term view with longer-term considerations of behavior and performance.

Not surprisingly, but reassuringly, COBIT was promoted as an excellent model to guide a company or department along the Good IT Governance path.

Thank you again to Ivan for this excellent seminar.

John Demsey, SICPA, Lausanne

Information Systems Audit and Control Association®

www.isaca.ch

Sechs spannende Kurse!

Internet Security Lab
Angriffszenarien und Abwehrmassnahmen
24. - 26. August 2005 in Zürich

Evidence Lab
Workshop über praktische Spurensuche in Computersystemen
7. - 9. September 2005 in Zürich

Application Security Lab
Sicherheit von Web-Anwendungen mit praktischen Beispielen
14. - 16. September 2005 in Zürich

Einführungskurs für SAP R/3
Systemhandling
30. August 2005 in Stuttgart

SAP R/3 Workshop
Workshop für Wirtschafts- und Informatikprüfer
31. August - 2. September 2005 in Stuttgart

Wirtschaftskriminalität
Krisenmanagement und Beweismittelsicherung
19. - 20. September 2005 in Zürich

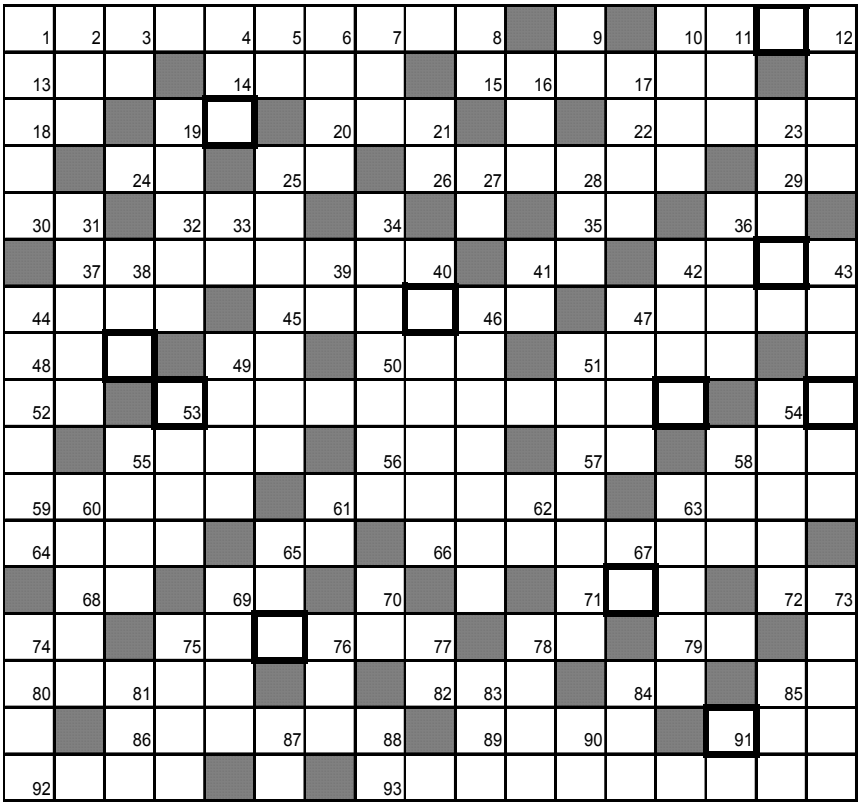
Weitere Informationen erhalten Sie in unserem Kurssekretariat:

ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40, 8006 Zürich, Schweiz
kurse@isaca.ch, Tel. 044 444 11 01, Fax 044 444 11 02

Information Systems Audit and Control Association

The ISACA Crossword Puzzle 3/05

Dieses Rätsel ist auf englisch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.



Across: 1 ***Easy to be hurt***; 10 stone edging pavement; 13 over the pond; 14 heavy club; 15 ***layer at back of eyeball***; 18 that is; 19 business unit; 20 and so on; 22 some type of ice hockey; 24 extra large; 25 it (G); 26 cylinder for holding thread; 29 soundless thorny flower; 30 German egg; 32 pub; 35 personal pronoun in the third case; 36 „double“ prefix; 37 embroidered initials; 41 ***information system***; 42 lacking colour; 44 pasteboard; 45 one dimensional; 47 tablets; 48 hand grid organization; 49 a short metropolis in the US; 50 personal possessive pronoun; 51 should rule over matter; 52 sure lost its consonants; 53 ***the classical method of identification***; 54 sound of enchantment; 55 ***extremity***; 56 Salinger saw the catcher there (i=y); 57 king (I); 58 to be heard at ***Corridas***; 59 deeply dark; 61 association football; 63 in a different way; 64 Ivy League university; 65 in triple: Santa is around the corner; 66 this one usually wins; 68 Finnish auto plate; 69 Babylonian earth god; 71 street in the Grisons; 72 short for Times Square; 74 Liliuokalani added this to Aloha for her immortal song; 75 wonder at; 78 infamous double consonant; 79 intelligence quotient; 80 big; 82 former Portuguese possession in India; 84 year (F); 85 closed (G); 86 authorize; 89 river in Asia; 91 beautiful (F); 92 uncommon; 93 ***well protected places***.

Down: 1 ***sound uttered by mouth***; 2 Kriemhild's mother; 3 line printer; 4 Australian ostrich; 5 Heyerdahl's papyrus boat; 6 return failures in tennis; 7 monetary risk engagement; 8 he (Ger); 9 extra terrestrial; 10 stepfather (middle high German); 11 European bar code (abb); 12 young men; 16 low tide; 17 bird; 19 ***without the power of vision***; 21 core business; 23 pointed steel; 25 European country; 27 Russian river; 28 large car; 31 ***picture***; 33 negation; 34 could be a Spanish baker; 36 hairless; 38 gold (S); 39 laughed (F); 40 ***measurement system***; 41 go (S); 42 an eighth of a gallon; 43 avoid; 44 fat looking ; 46 way of looking (pl); 47 tree with needles; 49 loop of a chain; 51 ***reflecting piece (pl)***; 53 ***headpiece***; 54 vigilant; 55 division by two;58 number; 60 ***strong light beam***; 61 therefore; 62 short for East River; 63 once more; 65 back of thigh; 67 Greek letter (often used for small); 69 Nordic saga; 70 the Swiss still do not pay in EUR; 73 ***the core of being*** (pl); 74 French men eating giant; 75 Henry the Eights second; 76 sick; 77 for instance; 78 velvet (G); 81 air (Greek); 83 useful in a rowboat; 84 form of to be; 85 dutch water; 87 an ancient comics character; 88 entire force; 90 ancient cow; 91 origin of Basel II.

This puzzle is in English. The solution is in the marked fields. This solution is to be sent on a postcard to Max F. Bretscher, Oberrenggstrasse 8, CH-8135 Langnau a/A. Solutions will also be accepted at mbretscher@kpmg.com. The deadline is August 5, 2005. The winner gets a credit of US$ 50 for reading material from the ISACA bookstore.

If there are less than 5 answers or the solution is not found, the US$ 50 go into the Watson Jackpot to be carried forward to the next issue of the ***NewsLetter***. Watson; There is some anomaly in each crossword puzzle. If detected, the Jackpot s emptied and the winner gets its content in similar credits at the ISACA bookstore.

Lösungen aus Nr. 74

Lösung Crossword Puzzle 2/05:
Lesefiehler

Waagrecht: 1 ***Byte***; 4 lockst; 9 ***IT***; 11 sub; 14 Rad; 15 Oel; 16 Kanu; 18 Aetna; 19 Ar; 20 Ski; 21 skurril; 23 (A)etn(a); 24 Udet; 26 Bit; 26 Bestien; 29 ICE; 31 Tobago; 34 LNM; 35 Au; 37 Knospe; 38 unsere; 40 Uhl; 42 Wunder; 44 roi; 46 tut; 49 fern; 50 Nro; 52 BL; 54 ***Verfuegbarkeit***; 57 Zu; 59 Ref; 60 Lear; 61 Los; 63 Rho; 65 Gewinn; 69 Ras; 71 Baltic; 72 ***Uptime***; 75 CC; 76 Aal; 78 ***Messen***; 80 tio; 82 Roadmap; 84 Lob; 86 Efeu; 88 Ort; 89 Energie; 92 EUR; 94 re; 95 UTENN; 96 rien; 97 dir; 98 Ast; 99 Nan; 101 ankern; 192 Satz.

Senkrecht: 1 Braunau; 2 ***Yard***; 3 TD; 4 Leib; 5 OL; 6 KKK (Ku Kux Klan); 7 Sauna; 8 Tnr; 10 Talsperre; 11 steiler; 12 unten; 13 Bannmeile; 15 OK; 17 Urbond; 20 St(o)ck; 21 Stop; 22 ie; 25 Ei; 27 Itsy; 30 eng; 32 bewegen; 33 Gunnar; 36 UHT; 39 Senke; 41 Luv;43 Urbanus; 45 Ob; 47 Ter; 48 Effet; 49 felice; 51 oil; 53 ***Turnaroun(d);*** 55 Reglement; 56 Tor; 58 ZH; 62 sac; 64 Oblate; 66 Wimper; 67 into; 68 Amt; 70 Schuetz; 73 Pele; 74 Eier; 77 Aorta; 79 Sagen; 81 Of; 83 an; 85 Bein; 87 erst; 90 Ria; 91 ink; 93 Ur; 97 Dr; 98 Aa.

Das Lösungswort hätte natürlich ***Lesefehler*** sein sollen. Das I war überflüssig. Damit ist der Jackpot wieder einmal geleert. Die Gewinner sind Jakob Kaufmann und Marc Bucher, die je US$ 75 in Gutschrift für Bezüge von ISACA bookstore gewinnen. Herzliche Gratulation!

In eigener Sache

Bei der Umstellung auf ein neues Titelblatt des ***NewsLetters*** ist uns ein böser Fehler unterlaufen: Die Nummer der Ausgabe wurde zweimal vorgeschaltet. Auf die Nummer 71 („Deutschland“) folgte die Nummer 73 (Sarbanes Oxley / Basel II). Einige wenige aufmerksame Empfänger des ***NewsLetters*** habe dies sofort bei Erhalt der Nummer 73 bemerkt und die Nummer 72 verlangt.

Autsch! Was tun? Die Alternativen sind:

- Es gibt keine Nummer 72
- Die Nummer 72 wird nachgeholt

Beide Varianten haben Nachteile. Im ersten Fall muss immer erklärt werden, weshalb die Nummer 72 fehlt. Ausserdem ist es eine heikle Sache mit den „runden“ Jubiläumsnummern, die entweder zum falschen Zeitpunkt oder mit der falschen Nummer herauskommen werden. Im zweiten Fall wäre die Chronologie nicht eingehalten. Fazit: Alles falsch.

Wir haben uns für den ersten Fall entschieden. Damit bleibt der eine Fehler bestehen und es kommt nicht noch ein zweiter dazu. Eine spätere Redaktion kann dann immer noch entscheiden, eine Nummer 72 sozusagen als Witzblatt mit lauter leeren Seiten irgendwann einzustreuen, um die fortlaufende Numerierung wieder herzustellen.

Auf jeden Fall kann uns mit Recht vorgeworfen werden, dass wir vielleicht auf drei, aber nicht richtig auf hundert zählen können. Und dies alles unter dem Thema EDV-Revision! Die Asche haben wir uns bereits auf das Haupt gestreut. Aber es hat nichts genützt.

Das Redaktionsteam

Express Line

A Word from the Chair

Greetings!

Are you looking for speaker ideas? Visit ***www.isaca.org/chaptereducation*** to use a new consolidated web page that allows you to easily browse other ISACA chapters' education pages to see what speakers and topics your fellow chapters are planning. Program and education chairs can also connect with chapter peers in their geographic region at ***www.isaca.org/chapterreports***.

As you are aware, the annual ISACA membership purge took place in April, so any memberships that were not renewed have now expired. These individuals will receive an exit survey and one last chance to renew.

Sunil Bakshi
Chair, Membership Board

Conference Spotlight

IT Value: Delivering on the Promise

This half-day session will be held in beautiful Oslo, Norway, on Wednesday, 22 June 2005. Discussion will center on the latest IT Governance Institute publication for enterprise leaders and boards of directors, ***The CEO's Guide to IT Value @ Risk***. The publication provides high-level guidance on the essential aspects of effective IT governance – ensuring value, mitigating risk, planning and execution.

John Spangenburg, Ph.D., chairman and founder of SeaQuation, will present an enlightening case study on how ING measures IT value delivery. John Thorp, president of Thorp Network Inc. and principal researcher for Fujitsu and DMR, will discuss best practices for IT value delivery, benefit realization and program portfolio management. This event is offered on a complimentary basis to C-suite level executives only. ISACA members planning to attend the International Conference are encouraged to invite a member of their C-suite to attend this event. Online registration and additional details are available at ***www.isaca.org/itvalue***.

Certification Update

ISACA will offer the CISA and CISM twice annually beginning in December of this year. Exam locations for the December 2005 administration will be limited primarily to large test sites (75 or more candidates/year) and languages with 500 or more candidates/year.

Specific details will be provided soon to ISACA leaders, members and exam candidates.

New CISM Job Practice Analysis Continues

A CISM job practice analysis study to update the criteria used to certify and examine CISM candidates was initiated in January.

An initial task force meeting resulted in changes to the current delineation. Subsequent focus panels and subject matter expert reviews are being held to further refine and validate the work.

To participate in focus panels or serve as a subject matter expert for future reviews, please contact Ron Hale at ***rhale@isaca.org*** or +1.847.590.7492.

News Briefs

ISACA's Career Centre Available in May!

The Career Centre will be available in May 2005 for IT professionals seeking to hire and those searching for a job.

ISACA members will be able to look for jobs online and specify criteria to limit each search. Job seekers will be able to search by geography, professional certification, experience level and a number of other factors. We encourage you to check ***www.isaca.org/jobs*** to be among the first to post your résumé in the ISACA members-only résumé database. Members will have the added advantage of being able to receive e-mail notification when new jobs are posted.

For those seeking to hire, the ISACA Career Centre will be ***the*** source for IT audit and information security professionals. The Career Centre will highlight the CISA and CISM designations, thus providing a special opportunity for those interested in hiring CISA or CISM holders.

Please visit ***www.isaca.org/jobs*** to explore this exciting new offering!

DACH-News

D: Aktivitäten des German Chapters

In den letzten Monaten wurde im Hintergrund intensiv von unserem Vorstandsmitglied Heinrich Geis an dem neuen Webauftritt des ISACA German Chapter gearbeitet. Nun ist es soweit und unsere neue Homepage ist online. Die Adresse hat sich nicht geändert, die Seite ist weiterhin unter www.isaca.de zu finden. In der nahen Zukunft wird es noch weitere Neuerungen inhaltlicher Art auf unserer Seite geben, aber wir wollen natürlich nicht zu viel vorwegnehmen – schauen Sie einfach ab und an einmal vorbei.

Da CobiT im letzten und diesen Jahr immer mehr an Popularität gewonnen hat, haben wir zwei wirklich interessante Angebote mit professionellen Seminarveranstaltern zum Thema CobiT ausgehandelt. Die beiden Veranstalter sind Management Circle sowie Serview mit einem ein- bzw. zweitägigen Seminar. Auch für weitere Seminare des Anbieters Serview haben wir entsprechende Rabatte ausgehandelt. Weitere Informationen hierzu finden Sie auf unserer Website.

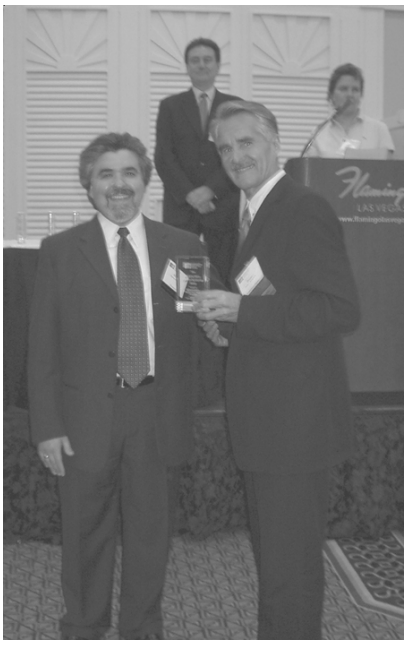
Unsere CISA-Kurse sind auch dieses Jahr wieder erfolgreich in Frankfurt und Mannheim gelaufen. Erstmalig wurde das Testexamen neben Frankfurt auch in Hamburg angeboten. Allen CISA-Kandidaten drücken wir für die bevorstehende Prüfung die Daumen und hoffen, dass die Ergebnisse unserer Teilnehmer so erfolgreich wie in den Vorjahren sein werden.

Ingo Struckmeyer
Vorstand German Chapter

CH

Global K. Wayne Snipes Award 2004 für die Schweiz

Anlässlich der Leadership-Konferenz in Las Vegas vom 23. und 24. April 2005 durfte der Delegierte des ISACA Switzerland Chapters gleich zwei K. Wayne Snipes Awards entgegennehmen. Vor rund 200 eingeladenen ISACA-Chapter-Präsidenten und Vertretern aus aller Welt wurde am 23. April der „Regional Award“ (Europa/Afrika) durch den internationalen Präsidenten, Marios Damianides (im Bild, links) an Bruno Wiederkehr, Vorstandsmitglied des ISACA Switzerland Chapters überreicht.



Der Gewinner des „Global Award“ mit Zertifikat (weltweite Auszeichnung) wurde bis zum 24. April streng geheim gehalten. Dann war es soweit: Im Hotel Flamingo überreichte Professor Alan T. Lord (im Bild, links) den Global K. Wayne Snipes Award 2004 dem ISACA Switzerland Chapter unter grossem Applaus! Welch eine Überraschung und Ehre für die Schweiz!

Originaltext
„In recognition of outstanding performance during 2004, the Membership Board 2005 from the international Headquarter offers the K. Wayne Snipes Award and Certificate for ISACA Switzerland Chapter as the best very large chapter worldwide.“

Global & Regional (im Bild, links) K. Wayne Snipes Award 2004

Was ist der K. Wayne Snipes Award?

Jedes Chapter muss dem ISACA „US Headquarter“ jährlich einen Aktivitätsbericht abliefern, der Details zu folgenden Themen beinhaltet: Mitgliederversammlung, Vorstandssitzungen, Newsletter, Website, Ausbildung, Vor-

träge, Verbindungen zu anderen Vereinigungen, spezielle Aktivitäten für die Mitglieder, etc. Der Jahresbericht wird jeweils nach der Mitgliederversammlung eingereicht und gilt automatisch als Grundlage für das Auswahlverfahren zum besten Chapter (170) in der jeweiligen Grösse und im jeweiligen Erdteil. Mit steigender Mitgliederzahl (> 600) gehört die Schweiz seit Ende 2004 zu der Kategorie „Very Large Chapter". ISACA hat insgesamt rund 50 000 Mitglieder weltweit. Aus den Gewinnern pro Erdteil wird dann ein weltweiter Gewinner ausgewählt.

Wir freuen uns riesig über diese Anerkennung und leiten die Glückwünsche gerne weiter an den gesamten Vorstand und die Beauftragten/Helfer, alle Mitglieder, Personen mit Spezialaufgaben im Zusammenhang mit ISACA, sowie an die Speaker, Sponsoren, Aussteller und Helfer, welche an der europäischen Konferenz „EuroCacs 2004" in Zürich mitgewirkt haben.

Besonders zu erwähnen sind auch die professionelle Ausbildung, Zertifizierung und gute Abschlussquote der CISA und CISM in der Schweiz. Weitere Kurse, Seminare, Veranstaltungen und der Award 2003 für die zweitbeste ISACA Website zeigen das besondere Engagement des ISACA Switzerland Chapters.

Um auch in Zukunft zu den Besten zu gehören, ist die Steigerung der Leistungen hinsichtlich Leadership, Membership, Public Relation, Ausbildung, Koordination und Kommunikation weiterhin unerlässlich. Wir haben bereits Verbesserungen vorgenommen (Website, ***NewsLetter***-Erscheinungsbild, After-Hour Seminare, etc.) und sind dabei, weitere Ideen umzusetzen. Natürlich hoffen wir auf Ihre Mithilfe und nehmen Vorschläge gerne entgegen. Wir freuen uns, die ISACA Switzerland Aktivitäten weiterhin spannend und zu Ihrem Nutzen gestalten und anbieten zu können.

Daniela Gschwend & Bruno Wiederkehr

Numerus Clausus für das After-Hour-Seminar?!

Die diesjährigen After-Hour-Seminare erfreuen sich steigender Beliebtheit. Ob es daran liegt, dass sie nicht mehr im Landesmuseum stattfinden, wo männiglich eine antike Verstaubtheit vermutet? Wohl kaum. Es sind wahrscheinlich die interessanten Themen, die geboten werden. Peter Bitterli musste angesichts der Tatsache, dass die Besetzung des Versammlungsraums an den feuerpolizeilichen Grenzen kratzte, ankündigen, dass in Zukunft kurzfristige Anmeldungen zur Teilnahme u.U. zurückgewiesen werden müssen. Reservieren Sie sich die Daten demnach frühzeitig!

Am 30. März 2005 präsentierte Urs Fischer seine Erfahrungen bezüglich des Einsatzes von CobiT bei der Swiss Life unter dem Titel ***Implementing IT Governance Using the CobiT Maturity Model*** in Form einer Case Study. Die anschliessende Diskussion wurde teilweise hitzig geführt, wobei Urs immer wieder konkrete Beispiele für das Vorgehen der Swiss Life und Rechtfertigungen für die angewandten „Durchschnittsmethoden" vorbringen musste. Die Adaption von CobiT stiess bei den „Puristen" unter den Teilnehmern teilweise auf Widerstand, doch konnte jedermann für seine praktische Umgebung wertvolle Hinweise mitnehmen.

Monika Josi stellte am 27. April 2005 die Einführung der weltweit gültigen Instrumente für die Umsetzung der Sarbanes-Oxley-Vorschriften in ihrer Umgebung vor: ***SOX IT in Novartis***. Beeindruckt hat dabei das Tempo, mit welchem die Arbeit erledigt werden musste. Der Vortrag machte glaubhaft, dass der Buchstaben auch wirklich gelebt wird. Dazu ist es aber unerlässlich, dass einerseits das Top Management voll hinter der Sache steht (Aussagen, wie „Danke, dass Ihr an uns gedacht habt, aber wir möchten vorläufig lieber nicht mitmachen" werden von höchster Stelle abgeschossen) und eine straffe Disziplin gefordert wird (Lieferung von Tonnen von Papier genügt nicht). Bereits ist die zweite Runde der Verifizierung im Gang, wobei die ursprüngliche Selektion der Länder und Unternehmungen ausgedehnt wird.

In beiden Fällen muss festgestellt werden, dass die Umsetzung der Instrumente teuer ist. Neben den reinen Projektkosten muss der durch die Betroffenen selbst zu leistende Aufwand nicht übersehen werden. In beiden Fällen handelt es sich um Grossfirmen, die „sich dies leisten können," doch was tut die KMU?!

Am 25. Mai 2005 informierte uns Matthias Oswald zum Thema ***Sicherheit in gehosteten Voice-over-IP-Lösungen***. Dabei nannte er 15 Gefahrenherde, welche die Sicherheit beeinträchtigen können. Erschreckend war dabei, dass die Technologie und „wir" aus den Erfahrungen mit dem Internet wenig gelernt haben, und alle dort gemachten schmerzlichen Erfahrungen erneut auf uns zuzukommen scheinen. Dennoch glaubt männiglich, dass dieser Technologie (solange sie praktisch „gratis" zu haben ist) die Zukunft gehört.

Die nächsten After-Hour-Seminare dürften wiederum interessante Aspekte aus der Praxis zeigen. Ganz abgesehen davon, dass der ***Continuing Professional Education Credit*** sicher auch gebraucht werden kann.

Max F. Bretscher

News aus den Interessengruppen

IG Operational IT-Risk

Peter R. Bitterli
Bitterli Consulting AG
Stampfenbachstr. 40
8006 Zürich
Tel. + 41 44 444 11 01
Fax. +41 44 444 11 02
prb@bitterli-consulting.ch

Die Interessensgruppe „Operational IT-Risk“ hat sich in den vergangenen Monaten intensiv mit der Frage beschäftigt, welche (IT-) Sicherheitsanforderungen in den verschiedenen Gesetzen und Verordnungen (Basel II, EBK-Richtlinien, HIPAA, CFR 11, EU Datenschutzgesetz, DSG und VDSG usw.) vorkommen. Die Arbeit hat zu ein paar interessanten Erkenntnissen aber wenig direkt in die Praxis umsetzbaren Ergebnissen geführt.

Die Interessengruppe „Operational IT Risk“ plant in der jetzigen Phase eine Kochbuch-ähnliche Anleitung für das Management von IT-Risiken, welche vor allem für KMU, für Unternehmen ohne grosse Sicherheitsanforderungen an die IT oder für die ersten Schritte in ein umfassenderes IT-Risikomanagement (analog CobiT Quickstart) gedacht ist. Für diese zweite Phase werden noch zwei bis drei neue Mitglieder gesucht; arbeitswillige Personen mit genügend Zeit sollen sich bitte (erneut) an den IG-Leiter wenden.

IG Government IT-Audit („Closed user group“)

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

La participation à ce groupe est réservée aux collaborateurs des organes de contrôle.
Le groupe se concentre sur l’échange d’information sur des projets communs Confédération-cantons, l’organisation d’audits conjoints et l’élaboration de directives à l’attention des organes informatiques.
Prochaine séance : le 7 juin à Berne

IG Computer Forensics

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe-Motta 50
1211 Geneva 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
Mobile: +41 79 220 54 07
Paul.Wang@ch.pwc.com

L’objectif de ce groupe de discussion lié aux « Computer Forensics », est de fournir un forum d’intérêt et d’information sur les méthodologies et les outils de ce qu’on appelle communément en français « Assistance informatico-légale ». Ce forum offre la possibilité de partager des idées, des technologies, des outils et certainement aussi des notions juri-diques de ce domaine en constante évolution. Ce groupe de discussion abordera également des discussions techniques et procédurales sur les prérequis en matière de recherche de preuves informatiques. Même si les participants doivent être familiers avec la recherche, l’acquisition et l’analyse de preuves informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT-Governance

Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@ch.ey.com

Nächste Sitzung: Voraussichtlich Juni/ Anfang Juli
Weitere Interessenten können sich bei Rolf Merz anmelden.

Traktanden:
1. Präsentation der beiden Pilotprozesse PO1 und PO10
2. Festlegen Weiteres Vorgehen
3. Themen, Ziele und Organisation der nächsten Sitzung

IG Romandie

Vacant : touts personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s’annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

IG Outsourcing/Insourcing

Ulrich Engler
Swiss Life
CF/REV HG 3151
General-Guisan-Quai 40
Postfach, 8022 Zürich
Telefon +41 43 284 77 58
Telefax +41 43 284 47 33
ulrich.engler@swisslife.ch

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Mögliche Themen: Kontiniuität des Insourcers, Abhängigkeit vom Insourcer (Konkurs), Überarbeitetes Rundschreiben EBK, Fernwartung, etc.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@ch.ey.com

Nach einer längeren Pause hat die IG ihre Arbeit wieder aufgenommen.

- Wrap-Up/Standortbestimmung

Es wurden alle bisher erstellten Dokumente aufgelistet und sofern sie noch finalisiert werden müssen, einem Verantwortlichen zur Bearbeitung zugeteilt.

- Weiteres Vorgehen

Das Referenzmodell und die Risiko-Matrix sollen als Resultat der Phase I (Datenextrakt und Load) nochmals überarbeitet und bereinigt werden. Danach sollen sie auf der Website der ISACA öffentlich zugänglich gemacht werden. Die diversen Fact-Sheets werden zum Teil nochmals überarbeitet zum Teil neu erstellt und gelten als Resultat der Phase II (Projektvorgehen und weitere relevante Aspekte).

- Wahl des neuen IG Leiters

Nach einer kurzen Besprechung ist der bisherige IG Leiter bestätigt worden. Es findet somit keinen Wechsel statt.

- Diverses

Die Resultate sollen im Rahmen einer ISACA-Abendveranstaltung präsentiert werden.

Nächste Sitzung: Mittwoch, 28. Juni 2005, 09.30 bei Ernst & Young AG, Bleicherweg 21, Zürich
Traktanden:

- Verabschiedung der Resultate aus Phase I
- Diskussion der Fact Sheets
- Diverses

ev. gemeinsames Mittagessen

Neue Interessenten können sich bei Daniel Oser, IG-Leiter, anmelden.

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijoustrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Nächste Sitzung: 28. November 2005 in Bern, bei der Eidg. Finanzkontrolle, Monbijoustrasse 45, 09.45–16.45 Uhr ***(bitte anmelden)***
Traktanden:

- Fachpräsentation
- Erfahrungsaustausch
- gemeinsames Mittagessen, dann Führung durchs Parlamentsgebäude und anschliessend auf der Tribüne Miterleben der Herbstsessionseröffnung des Nationalrates ***(Personalausweis mitbringen)***

Neue Interessenten können sich bei Monika Galli, IG-Leiterin, anmelden.

Eine Revisorin stand verzweifelt am Zoll,
Weil sie sich biometrisch ausweisen soll.
Sie verlor jeden Anstand
Und machte den Handstand.
Die Zöllner fanden es lustig und irrsinnig toll.

There was an old audit girl who was also a singer.
She worked very fast and hardly ever did linger.
When asked to produce her voice,
She made a remarkable choice,
She produced her tongue and an indecent finger.

Veranstaltungen

Anwendungssicherheit: Risikoorientierte Entwicklungsmethoden	6.–10. Juni 2005 Zürich, 5 Tage, ISACA/ITACS
Zutrittskontrolle im Spannungsfeld der Systemintegration	9. Juni 2005 Zürich, 1 Tag, Mediasec
2nd Annual CISO Executive Summit	16./17. Juni 2005 Genf, 2 Tage, MIS
IT-Sicherheitsseminar: Sicherheitskonzepte	16./17. Juni 2005 Sarnen, 2 Tage, Infosec
International Conference	19.–22. Juni 2005 Oslo, 4 Tage ISACA
Wirtschaftsspionage – Cyber Crime and Best Defence	24. Juni 2005 Zürich, 1 Tag, Infoguard
After Hour Seminar: Qualitätsmanagementsysteme und ihre typischen Schwächen	29. Juni 2005 16.40–17.40, Zürich, ISACA
Prüfung von Schnittstellen/Audit des Interfaces	30. Juni 2005 Bern, 1 Tag, ISACA/Kammer
CobiT Manager	4. Juli 2005 1 Tag, Frankfurt, Management Circle
CobiT Manager, IT Governance in Practice	11./12. Juli 2005 2 Tage, Bad Homburg, Serview GmbH
CobiT Manager	1. August 2005 1 Tag, München, Management Circle
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	24.–26. August 2005 Zürich, 3 Tage, ISACA/Compass
Einführungskurs in Systemhandling für SAP R/3 Workshop	30. August 2005 Stuttgart, 1 Tag, ISACA
After Hour Seminar: Corporate & ICT Performance Management (CPM)	30. August 2005 16.40–17.40, Zürich, ISACA
SAP R/3 Workshop für Wirtschafts- und Informatikprüfer	31. Aug .–2. Sept. 2005 Stuttgart, 3 Tage, ISACA
PKI – Einführung in Public Key Infrastructures	5. September 2005 1 Tag, Zug, Infoguard
CobiT Manager	5. September 2005 1 Tag, Köln, Management Circle
Evidence Lab – Workshop über die Spurensuche in Computersystemen	7.–9. September 2005 Zürich, 3 Tage, ISACA/Compass
SSI-Fachtagung: Der neue und sichere Arbeitsplatz	13. September 2005 1 Tag, Zürich, MediaSec

Kontaktadressen Veranstalter

Der ***NewsLetter*** empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
Tel. +33 1 55 62 12 22
afai@afai.asso.fr
www.afai.asso.fr

advanced technology seminars
Grundgasse 13
CH-9500 Wil
Tel. +41 71 911 99 15
Fax. +41 71 911 99 16
Maurer@inf.ethz.ch

Stiftung für Datenschutz und Informationssicherheit
Dr. Beat Rudin
Kirschgartenstrasse 7
Postfach
CH-4010 Basel
Tel. +41 61 270 17 70
Fax +41 61 270 17 71
beat.rudin@privacy-security.ch
www.privacy-security.ch

e-tec Security
PO Box 54
Wilmslow Chesire SK9 6FU
United Kingdom
info@a-tecsecurity.com

Euroform Deutschland GmbH
Hans-Günther-Sohl-Strasse 7
D-40235 Düsseldorf
Tel. +49 211 96 86 300
Fax. +49 211 96 86 509
info@euroforum.com

Hochschule für Technik Rapperswil
Institut für Internet Technologien und Anwendungen
Oberseestrasse 10
8640 Rapperwil
Tel. +41 55 222 41 11
Fax. +41 55 222 44 00
office@hsr.ch

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@t-online.de

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Tel. +41 41 749 19 00
Fax +41 41 749 19 10
www.infosec.com

Integralis GmbH
Gutenbergstr. 1
D-85737 Ismaning
Tel. +49 89 94573 447
Fax +49 89 94573 199 fx
schulung@integralis.de

ISACA CH Kurssekretariat
c/o ITACAS Training AG
Stampfenbachstrasse 40
CH-80006 Zürich
Tel. + 41 44 444 11 01
Fax +41 44 444 11 02
prb@bitterli-consulting.ch

ISACA USA
3701 Algonquin Rd #1010
USA_Rolling Meadows IL 60008
Tel. +1 847 253 15 45
Fax. +1 847 253 14 43
www.isaca.org

ITACS Training AG
Stampfenbachstrasse 40
CH-80006 Zürich
Tel. +41 44 444 11 01
Fax +41 44 444 11 02
www.itacs.ch

Management Circle
Hauptstrasse 129
D-65760 Eschborn/Ts.
Tel. +49 6196 4722-800
anmeldung@managementcircle.de

Marcus Evans
Weteringschans 109
1017 SB, Amsterdam
The Netherlands
Tel. +31 20 531 28 13
Fax. +31 20 428 96 24
www.marcusevansnl.com

MIS Training Institute
Nestor House
Playhouse Yard P.O. Box 21
GB-London EC4V 5EX
Tel. +44 171 779 8944
Fax. +44 171 779 8293
www.misti.com

MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Tel. +41 1 360 70 70
Fax. +41 1 360 77 77
it@mediasec.ch

Secorvo Security Consulting GmbH
Secorvo College
Albert-Nestler-Strasse 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
info@secorvo.de
www.secorvo.de

Serview GmbH
The Business IT Alignment Company
Gartenstrasse 23
D-61352 Bad Homburg
Tel. +49 6172 177 44-0

Treuhand-Kammer
Jungholzstrasse 43
Postfach
CH-8050 Zürich
Tel. +41 1 305 38 60
Fax. + 41 1 305 38 61

ZfU Zentrum für Unternehmensführung AG
Im Park 4
CH-8800 Thalwil
Tel. +41 1 720 88 88
Fax. +41 720 08 88
info@zfu.ch

Vereinsadressen

Germany Chapter

Geschäftsstelle
ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
isaca.dinslaken@t-online.de

Präsidentin
Karin Thelemann
Tel. +49 6196 99626 488
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Tel. +49 69 9587 2313
MGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
Tel. +49 201 438 0
Norbert.Groening@de.pwcglobal.com

Public Relations
Heinrich Geis
Tel. +49 692 101 5149
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
Tel. +49 4106 704 2336
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Holger Klindtworth
Tel. +49 (40)41522863
h.klindtworth@susat.de

Austria Chapter

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand
Tel: +43 1 31332 656
m.schirmbrand@kpmg.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Tel: +43 1 53127 2857
maria-theresia.stadler@oekb.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner
PricewaterhouseCoopers
Tel: +43 1 501 88 1701
josef.renner@at.pwcglobal.com

Schriftführer, Mitgliederversammlung, Marketing
Mag. Gunther W. Reimoser
Tel: +43 1 12 111 701 032
gunther.reimoser@at.ey.com

Kassier, Webmaster
Mag. Jimmy Heschl
Tel: +43 1 31332 619
jimmy@heschl.at

CISA/CISM-Koordinator
Mag. Ulrike Knödlstorfer-Ross
Tel: +43 1 33151 145
ulrike.knoedelstorfer@ama.gv.at

NewsLetter-Koordination
Mag. Dieter Stangl-Krieger
Tel: +43 1 31332 619
DStangl-Krieger@kpmg.at

E-Mail ISACA Austria Chapter:
office@isaca.at
Homepage ISACA Austria Chapter:
www.isaca.at

Switzerland Chapter

Präsidentin
Daniela S. Gschwend
Tel. +41 43 285 69 36
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Tel. +41 31 323 10 35
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Tel. +41 71 626 64 61
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Tel. +41 44 444 11 01
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Tel. +41 44 421 64 22
tbucher@deloitte.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Tel. +41 61 697 72 41
monika.josi@novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Tel. +41 58 286 66 79
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Paul Wang
Tel. +41 22 748 56 01
paul.wang@ch.pwcglobal.com

Marketing
Bruno Wiederkehr
Tel. +41 1 910 96 33
bru.wiederkehr@bluewin.ch

Homepage ISACA Switzerland Chapter: www.isaca.ch