**Zeitschrift:** Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES

**Band:** 97 (2006)

**Heft:** 7

**Artikel:** Einfluss von Mitarbeitenden auf die Informationssicherheit

**Autor:** Schlienger, Thomas

**DOI:** https://doi.org/10.5169/seals-857662

**Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

**Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

**Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

**Download PDF:** 15.10.2024

**ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch**

# Einfluss von Mitarbeitenden auf die Informationssicherheit

## Effektive Informationssicherheit kann nicht alleine mit technischen und organisatorischen Mitteln erreicht werden

Das Thema Informationssicherheitskultur ist allgegenwärtig. War man noch vor der Jahrtausendwende der Meinung, dass Informationssicherheit allein durch fortschreitende technische und organisatorische Lösungen vorangetrieben werden könne, wächst heute zunehmend das Bewusstsein um den beachtlichen Einfluss menschlichen Verhaltens. Trotz dieses zunehmenden Bewusstseins ist die Sensibilisiertheit auf sicheres Verhalten im Alltag jedoch ungenügend.

*Thomas Schlienger*

Studien belegen, dass Mitarbeitende das grösste Hindernis für eine effektive Informationssicherheit sind [1, 2]. Das Mitarbeiterrisiko steht mit rund 55% auch an oberster Stelle der Sicherheitsrisiken, beispielsweise in Form von unbeabsichtigtem Fehlverhalten (z.B. das naive Anklicken eines E-Mail-Virus) oder von Fehlkonfigurationen an Servern und PCs. Konsequenzen können dabei der Ausfall der Verfügbarkeit von Informatikdiensten oder der Abfluss vertraulicher Daten sein. Der direkte Verlust ist dabei meist gross, eine CSI/FBI[1]-Studie [2] nennt im letzteren Fall einen durchschnittlichen direkten Schaden von rund 450 000 Franken, ganz zu schweigen von den kaum bezifferbaren indirekten Folgeschäden.

Trotzdem investieren noch immer nur die wenigsten Organisationen in die Sensibilisierung und Ausbildung ihrer Arbeitskräfte. Soll die Informationssicherheit umfassend gewährleistet werden, muss der Mensch als Benutzer der Informations- und Kommunikationstechnologie berücksichtigt werden. Nur mit einer ganzheitlichen Betrachtung der technischen, organisatorischen und menschlichen Aspekte kann Information effektiv und effizient gesichert werden. Hierfür ist eine tief gehende Beschäftigung mit den sozialen, kulturellen und ethischen Aspekten notwendig, die im Weiteren unter dem Konzept der Informationssicherheitskultur zusammengefasst werden.

### Was ist Sicherheitskultur?

Bei den Mitarbeitenden lässt sich ein ungenutztes Sicherheits-Potenzial feststellen. Deshalb wird seit Ende der neunziger Jahre die Institutionalisierung der Informationssicherheit vorangetrieben [3]. Diese berücksichtigt unter anderem auch sozio-kulturelle Aspekte der Informationssicherheit, die so genannte Sicherheitskultur.

Die Informationssicherheitskultur ist ein Bestandteil der Unternehmenskultur und bestimmt die Wahrnehmung, das Denken, Fühlen und Handeln in Bezug auf Informationssicherheit. Sie gehört damit zu den informellen Strukturen einer Organisation und wird hauptsächlich durch das Management der Organisation beeinflusst und im besten Fall sogar entwickelt.

Der Kern einer jeden Unternehmenskultur sind grundlegende Annahmen über die Natur der Menschen, ihr Verhalten und ihre Beziehungen. Diese Annahmen manifestieren sich in den kollektiven Normen, Werten und Wissensbeständen einer Organisation, welche dann letztlich in Form von Artefakten und Kreation wie Handbücher, Anekdoten oder Vorgehensweisen ausgedrückt werden und dabei einen Einfluss auf den Unternehmenserfolg haben. Die Unternehmenskultur ist ein wachsendes und sich änderndes kollektives Phänomen, welches verschiedene organisatorische und inhaltliche Subkulturen hat. Eine davon ist die Sicherheitskultur, sie unterstützt die täglichen Aktivitäten auf eine Art und Weise, dass Informationssicherheit ein natürlicher Aspekt in den täglichen Aktivitäten eines jeden Organisationsmitgliedes wird. Zudem hilft eine geeignete Sicherheitskultur, das nötige Vertrauen zwischen den verschiedenen Partnern innerhalb einer Organisation aufzubauen und zielt somit auf das «Mein Benutzer ist mein grösster Feind»-Syndrom ab. Bild 1 zeigt die drei Schichten der Unternehmenskultur exemplarisch auf.

Studien haben ergeben, dass die meisten Organisationen heute Informationssicherheitskultur fördernde Massnahmen einsetzen (Bild 2, [5]). Am meisten kommen dabei jedoch noch Weisungen zur Informationssicherheit zum Einsatz und zielen damit auf den rein organisatorischen Aspekt der Informationssicherheit ab. Bei der Frage, welche Massnahmen in Zukunft geplant sind, zeigt sich jedoch ein Wechsel weg von Weisungen hin zu Verständnis- und Sensibilisierungsmassnahmen. Vermehrt eingesetzt werden sollen kleine Geschenkartikel zur Sensibilisierung, wie z. B. Mausmatten mit Sicherheitssprüchen, Workshops zur Ausbildung, Wissenstests und Rundgänge zur Überprüfung des Wissens und des Verhaltens. Es zeigt sich also eine Bewegung weg von organisatorischen hin zu sozio-kulturellen Massnahmen. Die Problematik einer organisatorischen Überreglementierung in der Informationssicherheit, ohne für deren Verständnis bei den Mitarbeitenden zu sorgen, wird also heute von der Wirtschaft erkannt. Stattdessen soll in Zukunft mehr auf Eigenverantwortung und Eigeninitiative gesetzt werden.

Der positive Effekt einer Informationssicherheitskultur auf die Informationssicherheit wird heute von den Sicherheitsverantwortlichen nicht bestritten. Die Massnahmen werden heute jedoch noch ad hoc und in Einzelprojekten umgesetzt. Erst ein systematisches Management der

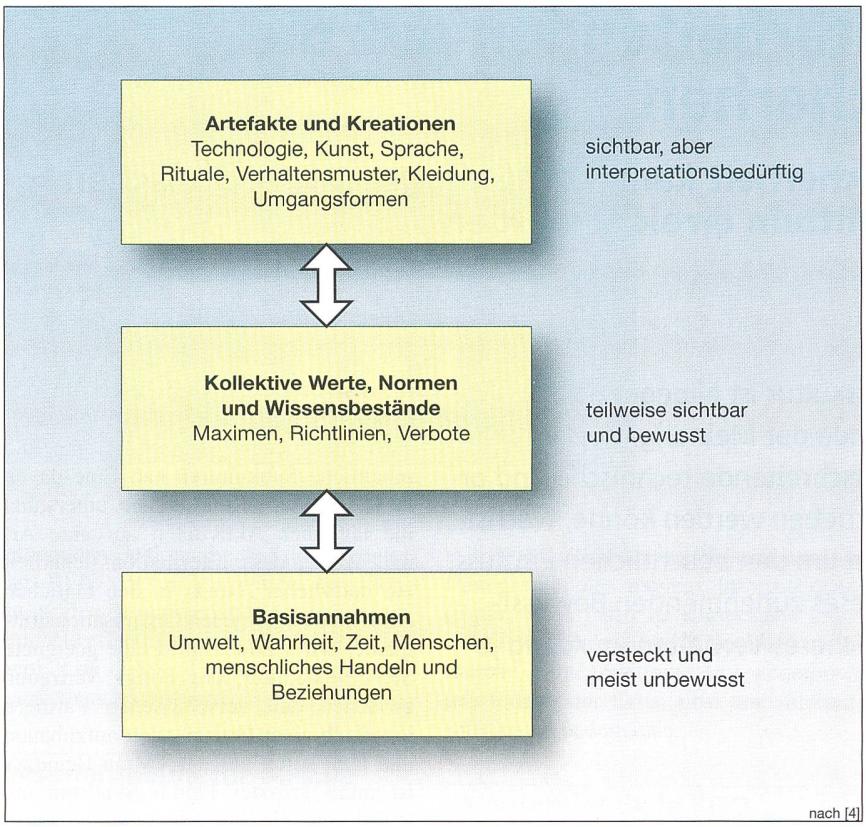


Bild 1 Die drei Schichten der Sicherheitskultur und ihre Interaktionen



Informationssicherheitskultur kann aber die gewünschten Effekte erzielen und damit die Investitionen rechtfertigen.

## Management der Sicherheitskultur

Informationssicherheitskultur ist kein einmaliges Projekt, sondern muss ständig analysiert, gefördert und angepasst werden. Man kann daher diese Aufgabe als einen Zyklus, wie er in Bild 3 dargestellt ist, betrachten. Das Modell orientiert sich am Information Security Management System (ISMS) des «ISO 27001:2005»-Standards [6]. In unseren Projekten wird der Prozess dabei grösstenteils durch ein internetbasiertes Managementsystem unterstützt, welches im Laufe des Forschungsprojektes am *international institute of management in technology* (iimt) der Universität Fribourg entwickelt wurde. Das Tool führt durch den Managementprozess, indem es einen Internetfragebogen und automatische Auswertungen für die Diagnose, Vergleiche mit sich selbst oder einem Benchmark, sowie die automatische Detektion von Schwachstellen in der Kultur mit Vorschlägen zur Verbesserung anbietet. Dank dieser Werkzeugunterstützung wurden Sicherheitskulturprojekte in kürzester Zeit mit wenig Personal erfolgreich durchgeführt. Die Projektpartner konnten so gezielt Massnahmen zur Verbesserung der Sicherheitskultur, wie beispielsweise Sensibiliserungskampagnen, Identitätsmanagement zur Abschwächung der Passwortproblematik, verbessertes Vorfallmanagement oder geeignetes Schulungs- und Ausbildungsangebot umsetzen. Diese Massnahmen haben durch die Kulturdiagnose ihre Berechtigung erhalten und konnten dabei das Sicherheitsniveau gezielt an den wichtigsten Punkten verbessern.

### 1. Schritt: die Diagnose des Ist-Zustands

Am Anfang eines gezielten Informationssicherheitskultur-Managements steht die *Diagnose* der Ausgangslage durch Aufzeigen der aktuellen Stärken und Schwächen.

Die Untersuchung von Organisationskultur wurde und wird immer noch in der Fachliteratur kontrovers diskutiert. Die Methoden aus diesem Forschungsgebiet können auch für die Sicherheitskultur verwendet werden, wobei wir von den gemachten Erfahrungen profitieren können.

Zwei Hauptströmungen lassen sich identifizieren. Auf der einen Seite befinden sich die so genannten Funktionalisten, die Kultur als objektiv messbares Konzept ansehen («die Organisation hat eine Kultur»). Zur Analyse bieten sich daher z.B. standardisierte Fragebogen an. Die Antworten können so zwischen verschiedenen Organisationen verglichen werden. Auf der anderen Seite sind die so genannten Interpretativisten, die Kultur als allumfassendes Konzept auffassen («die Organisation ist eine Kultur»). Kultur kann daher nicht anhand verschiedener Messpunkte objektiv gemessen, sondern nur anhand einer vollständigen Beobachtung aller Verhaltensweisen interpretiert werden. Als Methoden werden daher Beobachtung und Interviews angewendet.

In der Praxis bietet sich an, von den Erkenntnissen beider Strömungen zu profitieren und verschiedene Untersuchungsmethoden in Form eines Methoden-Mix zu verwenden:

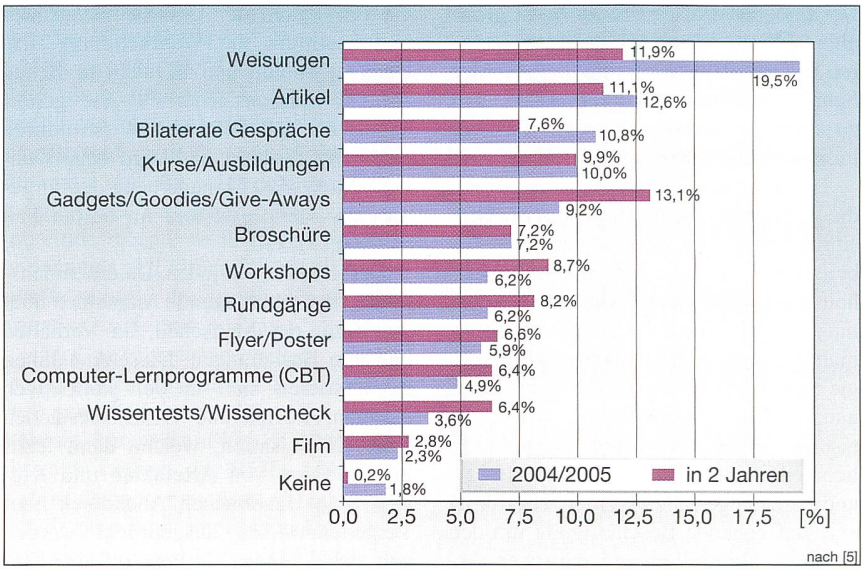


Bild 2 Sicherheitskultur fördernde Massnahmen heute und in Zukunft

- Analyse der Sicherheitspolitik
- Fragebogen an die Mitarbeiter
- Interview mit dem Sicherheitsverantwortlichen
- Objektive Messung von Verhaltensmustern.

Die Analyse der Informationssicherheitspolitik gibt Aufschluss über die offiziellen Werte der Organisation und über geforderte Verhaltensnormen. Der Internet-Fragebogen zielt hauptsächlich auf das Wertesystem, das Wissen und die Wahrnehmung der Mitarbeitenden ab. Die Diagnose der Antworten wird dabei vollautomatisch über das Internet abgewickelt und kann daher in sehr kurzer Zeit durchgeführt werden. Bild 4 zeigt eine beispielhafte Sicht auf die Hauptdimensionen des Fragebogens, die auf einen ersten Blick die aktuellen Stärken (100 Punkte) und Schwächen (0 Punkte) aufzeigen. In den meisten Fällen hat sich gezeigt, dass die offizielle Firmenpolitik die Einstellung der Mitarbeitenden massgebend prägt. Die Mitarbeitenden fühlen sich selbst für die Informationssicherheit verantwortlicher, wenn die Firmenpolitik ihnen diese Rolle auch zuschreibt. Zwängt jedoch die Politik die Mitarbeitenden in ein komplexes Regelwerk, stehlen sich die Mitarbeitenden oft aus der Verantwortung und schieben diese auf die Organisation, den Vorgesetzten oder die Arbeitskollegen ab. Jedes Diagnoseinstrument bietet an und für sich schon viele Informationen über die Informationssicherheitskultur, eine Verknüpfung der verschiedenen Bilder ermöglicht jedoch erst das tief greifende Verständnis der vorherrschenden Kultur.

### 2. Schritt: die Planung der Massnahmen

Nach der Diagnose kommt die *Planung* der Massnahmen, die die Informationssicherheitskultur verbessern sollen. Zuerst muss entschieden werden, wie die Soll-Informationssicherheitskultur aussehen soll und davon abgeleitet, welche Aspekte der Ist-Informationssicherheitskultur belassen, verbessert oder umfassend verändert werden müssen (Gap-Analyse[2]). Je nach Entwicklungsstufe der Informationssicherheitskultur genügen Anpassungen oder muss die Kultur radikal verändert werden. Ein Benchmarking mit dem Klassenbesten kann den Handlungsbedarf auch losgelöst eigener Vorgaben aufzeigen. Danach werden die Zielgruppen definiert und entsprechende Instrumente und Massnahmen ausgesucht und priorisiert. Auch die Massnahmenplanung wird durch die Internetapplikation unterstützt. Detektiert das Tool eine Schwäche in der Informationssicherheitskultur, schlägt es Massnahmen vor, die diesen Punkt verbessern können.

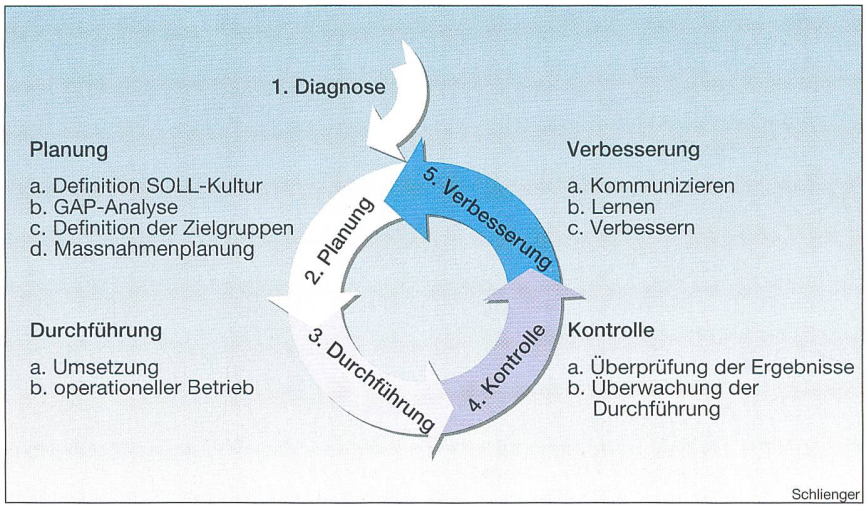


Bild 3 Managementprozess der Informationssicherheitskultur

### 3. Schritt: die Umsetzung der Massnahmen

In der *Durchführung* werden die geplanten Massnahmen in Projekten umgesetzt. Wichtig ist dabei vor allem eine durchgehende Unterstützung durch das Management und das Hinzuziehen von Fachspezialisten wie beispielsweise Kommunikationsexperten aus der eigenen Kommunikationsabteilung oder von extern. Wiederkehrende Massnahmen, wie etwa die Einführung neuer Mitarbeitender, werden in den operationellen Betrieb überführt.

### 4. Schritt: die Kontrolle der Massnahmen

In der *Kontrolle* wird die Durchführung der einzelnen Massnahmen überwacht und die erreichten Ziele durch Vergleichen des Zustandes vor und nach dem Informationssicherheitskultur-Programm evaluiert. Der Evaluationsprozess wird ebenfalls vollständig durch die Internetanwendung unterstützt und zeigt automatisiert die Veränderungen in der Informationssicherheitskultur auf.

### 5. Schritt: die Verbesserung der Massnahmen

Die letzte Phase, die *Verbesserung*, dient dazu, aus den gemachten Erfahrungen zu lernen, kurzfristig korrektive Massnahmen zu ergreifen und die eingesetzten Methoden und Instrumente zu verbessern. Ebenso sollten die erreichten Ziele und die Erfahrungen kommuniziert werden. Die Erkenntnisse aus dieser Phase fliessen dann in den nächsten Zyklus ein. Das Managementmodell stellt also an sich ein Lernprozess dar, der eine ständige und kontinuierliche Verbesse-

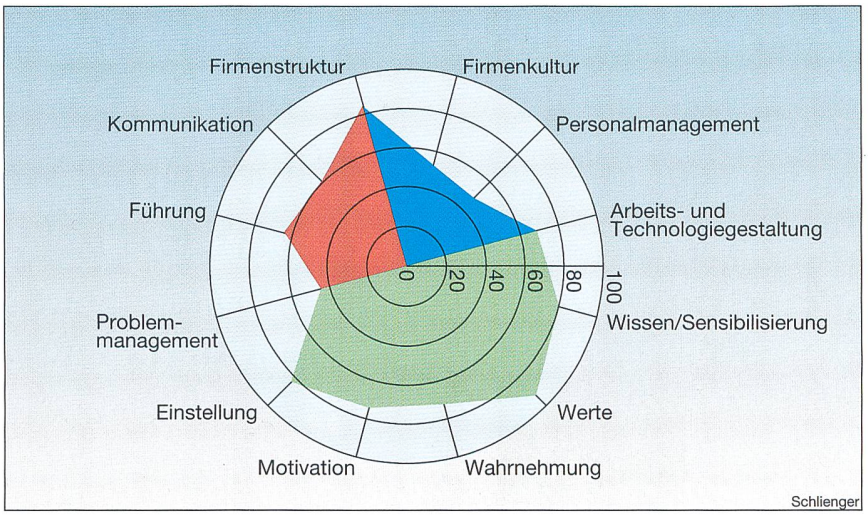


Bild 4 Diagnose der Informationssicherheitskultur

rung der Informationssicherheitskultur ermöglicht.

## Vom Sicherheitsrisiko zum Sicherheitsgaranten?

Informationssicherheit sollte zum Bestandteil unseres täglichen Lebens werden, sie sollte so natürlich wie Verkehrs- oder Gebäudesicherheit werden. Um dieses Ziel zu erreichen, braucht es eine Informationssicherheitskultur, welche auch die sozio-kulturellen Aspekte abdeckt. Die Mitarbeiter sollten zu Partnern in Fragen der Informationssicherheit werden und nicht nur als Sicherheitsrisiko betrachtet werden. Trotz Sicherheitskultur muss man jedoch realistisch bleiben, nicht allen Menschen kann und soll in allen Belangen vollumfänglich getraut werden, ein gewisses Risiko bleibt immer bestehen, welches mit technischen und organisatorischen Mitteln weiter eingeschränkt werden muss. Der Mitarbeiter wird immer beide Aspekte in sich vereinen: das Risiko und den Garanten. Tacitus hat aber noch immer Recht mit dem, was er schon vor zwei Jahrtausenden gesagt hat: «Der Wille zu schützen ist wichtiger als die Dicke des Schutzwalls.» Mit einem gezielten und systematischen Management ihrer Informationssicherheitskultur stärkt die Firma neben dem Willen auch die Fähigkeit zu schützen und legt damit einen unabdingbaren Grundstein für den Schutzwall des Unternehmens. Als praxisgerechte Vertiefung in die Thematik empfiehlt sich der von der Arbeitsgruppe «Informationssicherheitskultur» der FGSec (the information security society of switzerland) ausgearbeitete Leitfaden.

## Referenzen


[1] Deloitte, Global Security Survey. 2005, Deloitte Touche Tohmatsu: London.

[2] Computer Security Institute. 2005 CSI/FBI Computer Crime and Security Survey. 2005, Computer Security Institute (CSI). www.gocsi.com.

[3] B. von Solms: Information Security – The Third Wave. Computers & Security, 2000. 19(7): p. 615–620. Kluwer Academic Publishers.

[4] E. H. Schein: Organizational Culture and Leadership: A Dynamic View. 1985, San Francisco, Jossey-Bass.

[5] T. Schlienger, R. Rues Rizza: Befragung zur Informationssicherheitskultur in CH Organisationen. 2004, Arbeitsgruppe «Informationssicherheitskultur» der FGSec (information security society switzerland), www.fgsec.ch/ag/isk/Marktbefragung2p.pdf, 9.11.2004.

[6] ISO/IEC, ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements. 2005, International Organization for Standardization: Switzerland.

[7] T. Schlienger, C. Baur, et al.: Leitfaden zur Förderung und Analyse der Informationssicherheitskultur. FGSec Series, Hrsg. FGSec (information security society switzerland), 2004, Fribourg: iimt University Press.


## Angaben zum Autor


***Thomas Schlienger***, Dipl.-Inform., ist Doktorand am international institute of management in technology (iimt) der Universität Fribourg und Geschäftsführer der TreeSolution Consulting GmbH. Er ist Mitglied des Vorstands der Fachgruppe Security (FGSec) – the information security society of switzerland – und war Leiter ihrer Arbeitsgruppe «Informationssicherheitskultur».
*thomas.schlienger@treesolution.ch*


[1] CSI/FBI: Computer Security Institute/Federal Bureau of Investigation; www.gocsi.com, www.fbi.gov

[2] Die GAP-Analyse ist ein klassisches (quantitatives) Instrument der strategischen Planung. Mit ihr sollen strategische und zu erwartende Probleme rechtzeitig erkannt werden. Dazu liefert sie auf Basis mathematisch-statistischer Operationen rechnerische Ergebnisse bezüglich der zu prognostizierenden Grössen, mit denen die Differenz zwischen dem angestrebten Soll-Zustand und dem ohne zusätzliche Aktivitäten erreichbaren Zustand besteht.
Die Bezeichnung GAP-Analyse leitet sich von englisch Gap (= Lücke) ab. Sie wird daher auch als Lückenanalyse bezeichnet.


*Résumé*

## L'influence des collaborateurs sur la sécurité de l'information

*La sécurité effective des données ne peut être réalisée uniquement par des moyens techniques et organisationnels.* La culture de sécurité informatique est un sujet omniprésent. Mais tandis qu'avant le tournant du siècle on pensait pouvoir faire progresser la sécurité des données simplement par une technique et une organisation de plus en plus perfectionnées, on devient maintenant de plus en plus conscient du fait que le comportement humain exerce une influence considérable. Malgré cela, on n'est pas suffisamment sensibilisé aux questions de sécurité du comportement au quotidien.