Institut für Informatik der Universität Zürich

# Fallstudie zur Informationssicherheit

**Marcus Holthaus, Dr. Stephanie Teufel**

**Nr. 98.01** **Jan. 98**

# Fallstudie zur Informationssicherheit

*Marcus Holthaus, Dr. Stephanie Teufel*
*Institut für Informatik, Universität Zürich*
*Winterthurer Str. 190, CH-8057 Zürich*
*01 / 635 (45 80 | 43 35)*
*(holthaus|teufel)@ifi.unizh.ch*
*Version 1.1 vom 21. Januar 1998*

**Zusammenfassung**: Unternehmerische Informationssicherheit ist ein soziales und organisatorisches Problem, welches durch technologische Entwicklungen stark beeinflusst wird. Bei der Erhebung der Infrastruktur, bei der Massnahmenplanung und –umsetzung müssen deshalb verschiedene Interessengruppen innerhalb der Unternehmung mit einbezogen werden. Sie haben sehr unterschiedlichen Einfluss auf einen erfolgreichen Projektabschluss. Es entstehen Konflikte, welche der Beauftragte für Informationssicherheit erkennen und lösen muss. Nur so kann ein ganzheitliches Sicherheitskonzept erarbeitet und umgesetzt werden.

In dieser Fallstudie werden die organisatorischen und sozialen Probleme betrachtet. Dazu werden fünf Rollen definiert, welche von den Teilnehmern eines Workshops gespielt werden. Die Rollen sind in einer fiktiven Treuhand- und Revisionsgesellschaft angesiedelt und enthalten angenommene Meinungen und Verhaltensweisen des Geschäftsführers, der Leiter von Revision und Informatik, der Benutzer und des Informationssicherheitsbeauftragten.

Die Erfahrungen zeigen, dass sich die Fallstudie v.a. für Gruppen von 12 bis 25 Teilnehmern eignet. Die sozialen und psychologischen Probleme, welche die Erstellung und Umsetzung eines Sicherheitskonzepts mit sich bringen, treten deutlich zutage, während technische Aspekte weitgehend in den Hintergrund treten.

# Inhalt


**1 EINLEITUNG UND AUFBAU DER FALLSTUDIE ..... 4**

**2 VORAUSSETZUNGEN ..... 4**

**3 ABLAUF ..... 5**

**3.1 Vorbereitung ..... 5**

**3.2 Einleitung und Vorstellung der Rollen und des Ablaufs ..... 5**

**3.3 Gesprächsrunden mit Erarbeitung des Sicherheitskonzepts ..... 6**

**3.4 Präsentation und Diskussion ..... 6**

**4 MÖGLICHE ERWEITERUNGEN ..... 7**

**5 ERFAHRUNGEN ..... 8**

**6 ANHÄNGE ..... 9**

**6.1 Situationsbeschreibung und Auftrag Workshop ..... 10**

**6.2 Vorbereitung und Bereitstellung der Unterlagen ..... 11**

**6.3 Architekturskizze Informationssystem Gesamtsystem alle vier Firmen (jeweils nur Ausschnitt) ..... 12**

**6.4 Rolle des Geschäftsführers (GF) ..... 13**

**6.5 Informationssicherheitspolitik ..... 14**

**6.6 Rolle des Informationssicherheitsbeauftragten (ISiBe) ..... 18**

**6.7 Leitfaden für den Informationssicherheitsbeauftragten (ISiBe) ..... 19**

**6.8 Sicherheitskonzept TGAG ..... 21**

**6.9 Rolle des Leiters der Informatik-Abteilung (LInf) ..... 27**

**6.10 Architekturskizze Informationssystem TGAG (Ausschnitt) ..... 29**

**6.11 Rolle des Leiters der Revisionsabteilung (LRev) ..... 30**

**6.12 Rolle der Benutzer (Ben) ..... 31**

**6.13 Gesprächsrunden des Workshops ..... 32**

# 1 Einleitung und Aufbau der Fallstudie

Im Rahmen unserer Fortbildungsseminare in Informatik stehen wir immer wieder vor dem Problem, dass Informationssicherheit schlecht anhand praktischer Beispiele („hands-on“) vermittelbar ist. Zwar sind die technischen Aspekte (Einsatz von Firewalls, Analyse von Netzverkehr etc.) problemlos im Labor nachvollziehbar darzustellen, Informationssicherheit ist unserer Ansicht nach aber eine Managementaufgabe und deshalb nicht im Labor zu lehren. Die eher führungsorientierte Schulung von Informationssicherheitsbeauftragten unterscheidet sich also von der Schulung in konkreten Software- oder Hardwareprodukten. Ebenso unterscheidet sie sich von der konzeptionellen Arbeit an Informationsstrategien, da Informationssicherheit konkretere, personenorientierte Aufgabenstellungen verfolgt als eine (zumindest anfangs) technisch ausgerichtete theoretische Informatikstrategie. Gleichzeitig bestehen nur sehr wenige Fallstudien, welche sich für die Analyse im Unterricht eignen.

Aus diesem Grund haben wir eine fiktive Fallstudie entworfen, welche die von uns in der Projektarbeit gewonnen Erfahrungen bei der Erstellung und Umsetzung eines Sicherheitskonzepts widerspiegelt. Ihr Hauptbestandteil ist ein Rollenspiel, in welchem die Teilnehmer verschiedene Meinungen innerhalb einer Treuhand- und Revisionsgesellschaft vertreten. Eine der Rollen – die des betrieblichen Informationssicherheitsbeauftragten – wird von einer anderen Rolle – der des Geschäftsführers – mit der Erstellung eines Sicherheitskonzepts beauftragt. Er muss nun in vier Gesprächen mit den verschiedenen (weiteren) Rollen das Konzept von der Politik bis zum Massnahmenkatalog entwickeln, vorstellen und die Einführung planen. Weitere Rollen sind für den Leiter der Informatikabteilung, den Leiter der Abteilung Revision sowie Benutzer innerhalb der Unternehmung definiert.

Diese Fallstudie wurde von uns in verschiedenen Workshops im Rahmen von Fortbildungsseminarien verwendet und erzeugte durchwegs positives Echo. Sie wurde für eine Dauer von vier bis sechs Stunden entwickelt, wobei jeweils die Dauer der einzelnen Gesprächsrunden, die Tiefe der Präsentationen und die Möglichkeit der Koordination zwischen den einzelnen Rollenmitgliedern variiert wurde.

# 2 Voraussetzungen

Alle Teilnehmer bekommen eine einseitige Beschreibung ihrer Rolle sowie weiteres rollenspezifisches Dokumentationsmaterial, um im Verlauf der Gespräche die notwendigen Angaben (z.B. über technischen Aufbau der Informatikinstallationen) machen zu können. Um die Motivation hoch zu halten, wurden die Rollenbeschreibungen bewusst knapp gehalten. Ausserdem erhalten nicht alle Teilnehmer alle Informationen. Zudem sind die abgegebenen Anweisungen sind nicht konsistent – Konflikte sind also geplant.

Um das Rollenspiel zu gestalten, muss den Teilnehmern Zeit zur Verfügung gestellt werden, um ihre Rolle zu lesen und das Begleitmaterial zu überfliegen. Die Rollenbeschreibung enthält die wichtigsten Rahmenbedingungen der Rolle wie Aufgaben und Kompetenzen sowie Details aus der bisherigen Geschichte der Firma (z.B. sicherheitsrelevante Vorfälle). Da die Rolle aber nicht alle Details enthält, müssen die Teilnehmer diese bei Bedarf aus ihrer eigenen Berufserfahrung ergänzen. Bei der bisherigen Anwendung waren stets Informatiker und Betriebswirte mit mehrjähriger Berufserfahrung im Teilnehmerkreis, was die Diskussionen in den einzelnen Gesprächen anregte und von uns deshalb als Voraussetzung für die Durchführung angesehen wird.

Die ideale Anzahl Teilnehmer liegt bei etwa zwanzig. Notwendige Hilfsmittel zur Diskussion in den verschiedenen Runden sind drei bis fünf abgetrennte Räume mit Visualisierungshilfen (Whiteboard, Flipchart, Hellruamprojektor etc.) sowie Folien, auf welchen die Gruppen ihre Vorträge vorbereiten können. Jede Rolle wird durch eine Farbe identifiziert.

# 3 Ablauf

Die Fallstudie wird – nach einer Vorbereitung -- in drei Teilen bearbeitet:

- Einleitung und Vorstellung der Rollen und des Ablaufs
- Gesprächsrunden mit Erarbeitung des Sicherheitskonzepts
- Präsentation und Diskussion

## 3.1 Vorbereitung

Die Vorbereitung des Workshops umfasst die Behandlung der notwendigen Theorien zum Sicherheitsmanagement – insbesondere das Vorgehen für eine Sicherheitsanalyse – und die Bereitstellung der Unterlagen und von Hilfsmaterialien. Letztere sind in Abschnitt detailliert. Es ist nicht notwendig, die Fallstudie mit Vorlaufzeit abzugeben, z.B. um das Studium der Dokumente zur Hausaufgabe zu machen. Dies kann zwar hilfreich sein, jedoch nur, wenn die Teilnehmer während dieser Vorlaufzeit keinen Kontakt zueinander haben und sich nicht gegenseitig über die jeweiligen Rolleninhalte informieren können.

## 3.2 Einleitung und Vorstellung der Rollen und des Ablaufs

Zu Beginn des Workshops wird der gesamte Ablauf des Workshops und die Ausgangslage vorgestellt.

Die Situation, in welcher die Rollen angesiedelt sind, umfasst vier Firmen, welche geschäftliche Beziehungen untereinander pflegen. Im Zentrum steht die Treu & Glaub AG (TGAG), eine Revisions- und Treuhandgesellschaft, welche die Bücher der anderen Firmen führt bzw. deren externe Revisionsstelle ist (vgl. Abschnitt 6.1). Die TGAG hat einen Anschluss ans Internet beschlossen, um die geschäftlichen Beziehungen mit elektronischer Kommunikation noch intensivieren zu können und um ihr modernes Image zu unterstreichen. Eine mögliche Informatikstruktur unter Einbezug aller vier Firmen ist in Abschnitt 6.3 dargestellt.

Die Entscheidung, dass ein Internet-Anschluss vorgenommen werden soll, wurde vom Geschäftsführer (GF) getroffen (vgl. Rolle des Geschäftsführers in Abschnitt 6.4). Da er sich bewusst ist, dass dies Sicherheitsrisiken mit sich bringt, hat er einen Informationssicherheitsbeauftragten (ISiBe) bestimmt, der nicht nur die Sicherheit der Internet-Anbindung prüfen soll, sondern gesamthaft zu untersuchen hat, welchen Risiken die Informationsverarbeitung in der TGAG unterliegt. Damit ein grundsätzlicher Rahmen für die Nutzung der Informatik-Mittel entsteht, bringt der Geschäftsführer eine beinahe leere, neu erstellte Informationssicherheitspolitik (vgl. Abschnitt 6.5) in die Sicherheitsdiskussion ein, welche er mit Hilfe des Informationssicherheitsbeauftragten mit Regeln zu füllen beginnt.

Die Aufgabe des Informationssicherheitsbeauftragten (ISiBe) ist die Erstellung eines Sicherheitskonzepts. Er erhält neben seiner Rollenbeschreibung (vgl. Abschnitt 6.6) einen Leitfaden zur Erstellung von Sicherheitskonzepten (vgl. Abschnitt 6.7) und ein leeres Sicherheitskonzept, v.a. bestehend aus Tabellen zur Erhebung von Bedrohungen, Wahrscheinlichkeiten, Risiken und zur Festlegung von Massnahmen (vgl. Abschnitt 6.8). Im Rahmen der verschiedenen Gespräche muss er dieses Konzept mit Inhalten füllen. Er hat damit die tragende Rolle innerhalb des Workshops und die umfangreichste Aufgabe.

Viele der notwendigen Informationen erhält er von Leiter der Informatikabteilung der TGAG (LInf). Diese Abteilung sorgt für die interne Unterstützung mit Informatik-Hilfsmitteln und hat keine direkt ertragswirksame Aufgabe. Der Leiter der Informatik gibt gerne über die Infrastruktur und die ihm bekannten Unzulänglichkeiten im System Auskunft (vgl. Abschnitte 6.9 und 6.10).

Der Leiter der Revisionsabteilung, welche als externer Revisor anderer Firmen auftritt und damit direkt ertragswirksame Aufgaben hat, hat eine etwas andere Meinung zur Internet-Anbindung und zur Informatik-Unterstützung im Allgemeinen als sein Chef, der Geschäftsführer (vgl. Abschnitt 6.11). Allerdings ist der Leiter der Revisionsabteilung Mitglied der Geschäftsleitung, während es der Informatik-Chef nicht ist. Selbstverständlich wird die interne Informatik der TGAG nicht von der hausierenden Revisionsabteilung revidiert, sondern von einer anderen, nicht näher genannten Firma. Mit seiner abweichenden Meinung

macht der Revisionschef nicht nur dem Informationssicherheitsbeauftragten die Arbeit schwer, sondern auch seinen anderen Gesprächspartnern sowie seinem Chef.

Eine weitere Rolle spielen die Benutzer (vgl. Abschnitt 6.12). Sie kennen nur ihren eigenen Aufgabenbereich und haben nur wenig Interesse an oder Kenntnis von den übergeordneten Zusammenhängen. Sie können naive Züge aufweisen und ohne ihre eigene Erkenntnis entgegen Firmeninteressen handeln.

Im Rahmen des Workshops erhalten nun alle fünf Rollen Gelegenheit, mit jeweils allen anderen fünf Rollen Gespräche zu führen.

Dazu werden zuerst die Rollen verteilt. Diese sind, wie die dazugehörige Dokumentation, auf jeweils verschiedenfarbigem Papier gedruckt und zu (jeweils gleichfarbigen) Bündeln geheftet. Durch die Auslage dieser Papiere kann sich jeder Teilnehmer frei für eine Farbe und damit für eine Rolle entscheiden, wobei die Zuordnung zwischen Rolle und Farbe vorher bekanntgegeben werden kann, aber nicht muss. Da fünf Rollen vorhanden sind, sollte die Anzahl der verfügbaren Papierbündel pro Farbe gleich der aufgerundeten Anzahl der Teilnehmer geteilt durch fünf sein, um eine gleichmässige Verteilung zu gewährleisten. Zusätzlich erhält jeder Teilnehmer ein weisses Bündel.

## 3.3 Gesprächsrunden mit Erarbeitung des Sicherheitskonzepts

Nachdem allen Teilnehmern ca. 15 bis 30 Minuten Zeit gegeben wird, um ihre Rolle und die dazugehörenden Papiere zu lesen und Fragen dazu stellen – jedoch nicht, um sich gegenseitig zu informieren – beginnen die einzelnen Gespräche. Für jede Rolle ist dokumentiert, welchen Inhalt und welches Ziel die jeweiligen Gespräche haben sollten. In Runde 1 beispielsweise treffen sich Geschäftsführer, Leiter der Revision und Informationssicherheitsbeauftragter, um die groben Inhalte der Informationssicherheitspolitik festzulegen (1a). Da bei zwanzig Teilnehmern sich in diesem Fall zwölf Personen treffen, nämlich vier Geschäftsführer, vier Leiter der Revision und vier ISiBes, wird die Diskussion schwierig. Deshalb wird diese Diskussion (wie auch die anderen nachfolgenden mit mehr als zehn Personen) in zwei parallele Gruppen aufgeteilt, in welchen jeweils der gleiche Inhalt behandelt wird.

Parallel dazu treffen sich in der Runde 1 die verbliebenen Rollen Leiter der Informatik und Benutzer (1b). Hier geht es um die Feststellung der grundsätzlichen Anforderungen der Benutzer an die Informatik und um einen generellen Gedankenaustausch. Bei zwanzig Teilnehmern besteht diese Diskussionsrunde aus acht Personen und kann auch aufgeteilt werden, sofern Räumlichkeiten verfügbar sind.

Es ist essentiell, dass die beteiligten Personen nur ihre eigene Rolle kennen, deshalb durch die Argumentation des jeweiligen Gegenübers überrascht werden und darauf angemessen (diplomatisch oder weisend) regieren müssen.

Die Runde 1 sowie die weiteren drei Runden dauern jeweils 30 Minuten. Immer eine Rolle muss die Führung der Diskussion übernehmen, und jeder Teilnehmer ist gehalten, sich Notizen zu machen, um die abschliessende Präsentation vorzubereiten.

In Abschnitt 6.13 ist beispielhaft ein Zeitplan aufgeführt.

## 3.4 Präsentation und Diskussion

Zu Beginn von Runde 5 treffen sich jeweils alle Teilnehmer *derselben* Rolle, was bei zwanzig Teilnehmern fünf Gruppen zu je vier Personen ergibt. Ihre Aufgabe ist es nun,

- eine rollenspezifische Präsentation vorzubereiten. So muss
  - der Informationssicherheitsbeauftragte das Sicherheitskonzept darstellen,
  - der Geschäftsführer über Chancen und Risiken der Internet-Anbindung referieren,
  - der Leiter der Informatik über die geplanten technischen Sicherheitsmassnahmen und ihre Kosten sowie die Auswirkungen auf das Nutzungsumfeld sprechen,
  - der Benutzer darstellen, wie die Geschäftsleitung (GF und LRev) sowie die Informatik sie zu beeinflussen versucht haben und beschreiben, ob sie nun besser als zu Anfang motiviert sind,

    - der Leiter der Revision seine eigene Auffassung der Internet-Anbindung darlegen und seine ursprünglich kritische Haltung gegenüber der Vernetzung neu rechtfertigen oder aufgeben,
- darzustellen,
    - wie die anderen Rollen auf sie gewirkt haben,
    - was sie über Informationssicherheit und über die Konflikte bei der Erstellung von Informationssicherheitskonzepten gelernt haben, und
    - was sie entsprechend berücksichtigen oder verändern würden,
- aufzuzählen, wie realistisch der Workshop war, v.a.
    - ob Verhalten und Rollen realistisch definiert und gespielt wurden
    - wo Verbesserungspotential liegt.

Dazu stehen den Teilnehmern Folien und Stifte, möglichst viele verschiedene Räume (ideal: fünf) und 30 Minuten Zeit zur Verfügung. Jeder Teilnehmer kann die Ideen einfliessen lassen, welche er sich im Verlauf der vorherigen Runden notiert hat. Auch die Workshop-Leitung ist gehalten, sich Notizen anzufertigen und möglicherweise eine eigene kurze Präsentation vorzubereiten.

Eine abschliessende Diskussion ermöglicht die Behandlung der wichtigsten Punkte und die Klärung noch offener Fragen.

# 4 Mögliche Erweiterungen

Die drei weiteren Firmen, mit welchen die TGAG mit elektronischen Hilfsmitteln kooperiert, können ebenfalls in einen Workshop mit einbezogen werden. In einem konkreten Fall haben wir die Anhang 2 dargestellte Informatik-Infrastruktur physisch aufgebaut und technische Demonstrationen mit Hilfe dieser Installationen vorgenommen. So wurden in einem Workshop verschiedene Angriffe auf das unternehmensübergreifende Netzwerk simuliert und vorgeschlagene Gegenmassnahmen aktiviert. Dies umfasste die Verwendung von Pretty Good Privacy (PGP) zur Sicherung von vertraulicher und nachvollziehbarer Kommunikation (mitsamt Generierung von Schlüsselpaaren unter Verwendung des installierten E-Mail-Systems) sowie die korrekte Konfiguration eines Firewalls, um Angriffe von aussen zu unterbinden.

Als weitere Möglichkeiten denkbar sind die physische Analyse von Netzwerkverkehr, die Konfiguration der vorhandenen Sicherheitsmechanismen in den eingesetzten Betriebssystemen (bei uns bisher v.a. Linux, aber auch Windows NT) sowie die strategische Planung der Informatiksicherheit.

# 5 Erfahrungen

Unsere Absicht bei Konzeption und Durchführung des Workshops war es, zu demonstrieren, dass

- die Erstellung eines Informationssicherheitskonzepts eine grosse und wichtige Aufgabe ist, und die entsprechende Rückendeckung von den Entscheidungsträgern innerhalb der Unternehmung notwendig ist,
- in einer Unternehmung verschiedenste Meinungen vorherrschen können und dass
  - einzelne Weltbilder zu eng sind und nur einen Ausschnitt der Gesamtsituation erfassen (v.a. Benutzer),
  - einzelne Ansichten überholt sein können und Konflikte anlässlich der Sicherheitsuntersuchung ausbrechen können (v.a. Leiter der Revisionsabteilung),
  - ein ständiger Konflikt zwischen Benutzern und Informatiker von Unternehmungen bestehen kann, weil die Qualität der von der Informatikabteilung gegebenen Dienstleistung von beiden Seiten unterschiedlich beurteilt wird,
  - geschäftliche Entscheide unter Berücksichtigung der Chancen und Potentiale, möglicherweise aber in Unkenntnis der Risiken getroffen werden können,
- personelle Konflikte einen bedeutenden Einfluss auf die Erstellung und Durchsetzung eines Sicherheitskonzepts haben.

Die Teilnehmer beurteilten Aufbau und Inhalt des Workshops bisher als durchgängig realistisch (mit Ausnahme des knappen Zeitrahmens) und haben die Erreichung dieser Absichten bestätigt.

Wir konnten beobachten, dass Teilnehmer überdurchschnittlich oft Rollen wählten, welche in ihrem täglichen Berufsleben ihr Gegenüber sind. Informationssicherheitsbeauftragte haben oft die Rolle des Geschäftsführers gewählt, Informatik-Leiter die Rolle der Benutzer. Dies hat zum gegenseitigen Verständnis beigetragen und gemäss Aussage der Teilnehmer den Lerneffekt erhöht.

# 6 Anhänge

Die Anhänge sind jeweils alleine auf einer Seite gehalten, um ein einfacheres Kopieren und Verteilen zu erlauben. Die Anhänge enthalten:

- 6.1 Situationsbeschreibung und Auftrag Workshop
- 6.2 Vorbereitung und Bereitstellung der Unterlagen
- 6.3 Architekturskizze Informationssystem Gesamtsystem alle vier Firmen (jeweils nur Ausschnitt)
- 6.4 Rolle des Geschäftsführers (GF)
- 6.5 Informationssicherheitspolitik
- 6.6 Rolle des Informationssicherheitsbeauftragten (ISiBe)
- 6.7 Leitfaden für den Informationssicherheitsbeauftragten (ISiBe)
- 6.8 Sicherheitskonzept TGAG
- 6.9 Rolle des Leiters der Informatik-Abteilung (LInf)
- 6.10 Architekturskizze Informationssystem TGAG (Ausschnitt)
- 6.11 Rolle des Leiters der Revisionsabteilung (LRev)
- 6.12 Rolle der Benutzer (Ben)
- 6.13 Gesprächsrunden des Workshops

Die [Farbe] gibt an, welche Papierfarbe beim Kopieren verwendet werden sollte. Dies erleichtert die Zuordnung der Papiere zu den einzelnen Personen.

## 6.1 Situationsbeschreibung und Auftrag Workshop

Die Getränkehandlung „Flaschenpost“ (FlaPo), die Restaurantkette „Goldball“, die Treuhandgesellschaft Treu & Glaub AG“ (TGAG) und die Brauerei „Bierquell“ pflegen geschäftliche Kontakte untereinander:

- Die Brauerei beliefert die Getränkehandlung mit Bier,
- Die Getränkehandlung beliefert die Restaurantkette mit Bier,
- Die Treuhandgesellschaft erbringt Dienstleistungen für die anderen drei.

***Workshop-Auftrag: Sicherheitskonzept für Treuhand erstellen***

- Die Treuhand-Gesellschaft „Treu & Glaub AG“ (TGAG) hat 50 Mitarbeiter, welche in den Bereichen „Buchhaltung“ und „Revision“ Mandate betreuen. Unter anderem führt die TGAG die Finanzbuchhaltungen der Brauerei und der Getränkehandlung und ist die externe Revisionsstelle der Restaurantkette.
- Im Zusammenhang mit der anstehenden Internet-Anbindung der TGAG soll die Sicherheit der betrieblichen und im Auftrag verarbeiteten Informationen überdacht werden. Die Geschäftsleitung weiss, dass diese Informationen einen strategischen Wert haben und geschützt werden müssen.
- Der Geschäftsführer bestimmt einen Informationssicherheitsbeauftragten (ISiBe) [rot]. Dieser erstellt ein Sicherheitskonzept. Dazu führt er Interviews mit allen beteiligten Personen.
- Im Hause sind folgende Personen verfügbar und werden involviert:
  - der Geschäftsführer (GF) [grün],
  - der Leiter der Revision (LRev) [gelb],
  - der Leiter der internen Informatik (LInf) [blau],
  - Benutzer und Mitarbeiter (Ben) [orange],
- Jede dieser Personen hat ihre eigenen Aufgaben im geschäftlichen Alltag und verfolgt ihre eigenen Ziele. In den Interviews, welche der Sicherheitsbeauftragte [rot] mit den einzelnen Personen führt, werden deshalb Konflikte spürbar.

***Ziel und Anleitung zum Rollenspiel***

- Ziel des Rollenspieles ist es, die unterschiedlichen Auffassungen der betroffenen Personen und die daraus resultierenden Widerstände bei der Einführung von Sicherheit zu verdeutlichen.
- Entscheiden Sie sich für eine der fünf Rollen (ISiBe, GF, GRev, GInf, Ben).
- Sie erhalten eine Rollenbeschreibung, in welcher Ihre Ziele, Aufgaben, Verantwortungen und Kompetenzen kurz beschrieben sind. Lesen Sie Ihre Rolle mehrmals durch und spielen Sie sie ernsthaft, auch wenn sie nicht Ihren eigenen Überzeugungen entspricht. Nur so wird es spannend!
- Auf jeder Rollenbeschreibung steht, mit welchen anderen Rollen Sie sprechen sollten und welche Rolle die Gespräche jeweils leitet. Bestimmen Sie eine Person als Gesprächsleiter!
- Die Gespräche finden in vier Runden zu je 30 Min. statt und haben ein bestimmtes Ziel, welches auch auf dem Blatt mit der jeweiligen Rollenbeschreibung steht.
- Als Resultat des Workshops entsteht ein Sicherheitskonzept der TGAG.

## 6.2 Vorbereitung und Bereitstellung der Unterlagen

Es werden folgende Unterlagen benötigt:

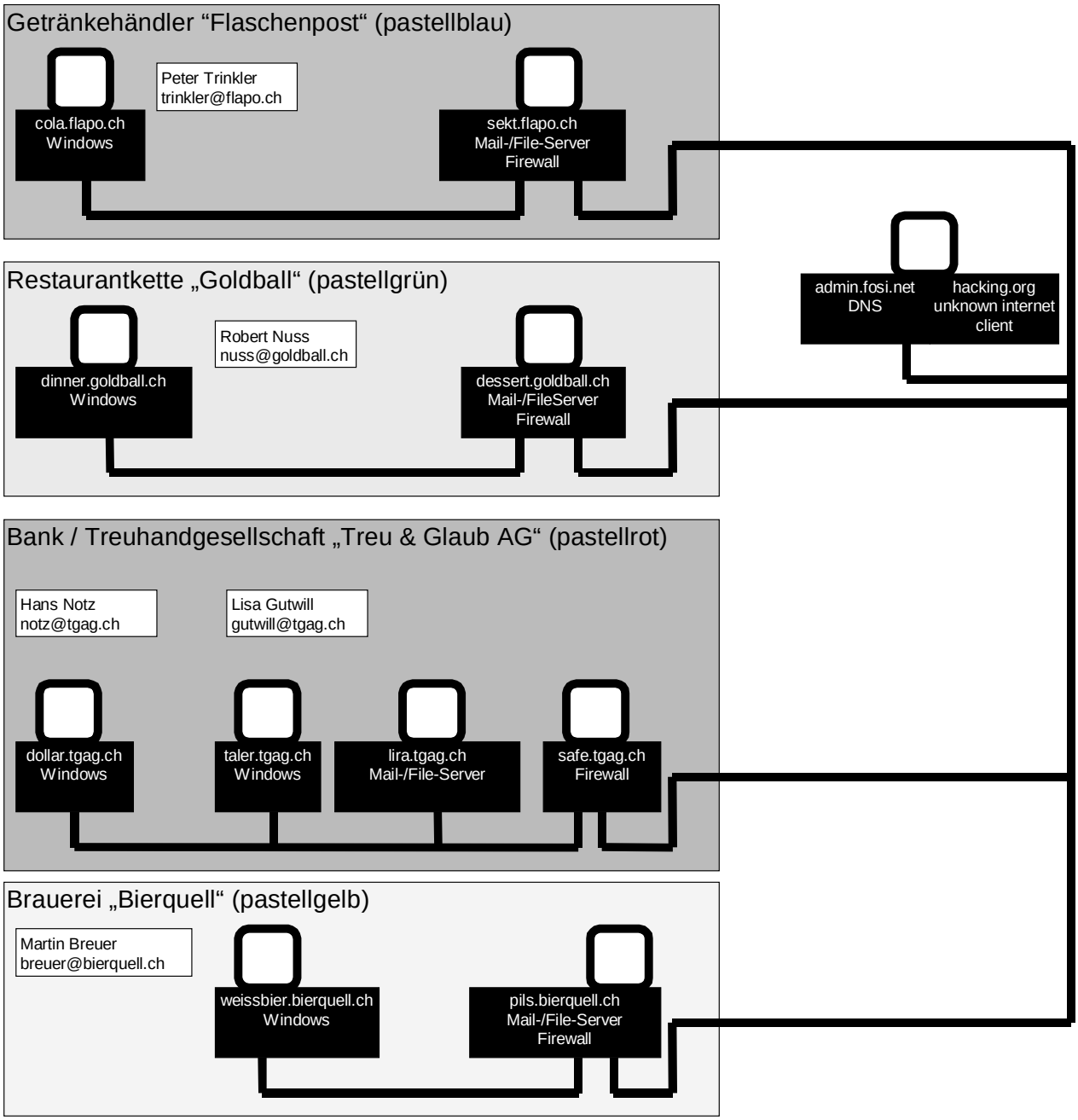
TN ist die Anzahl der Teilnehmer am Workshop, WL die Anzahl der Workshop-Leiter. Es sollte pro 10 Teilnehmern mindestens ein Leiter mitarbeiten.

| **Dokument** | **Farbe** | **Anzahl Exemplare auf Papier** | **Anzahl Folien** |
|---|---|---|---|
| Situationsbeschreibung und Auftrag Workshop | weiss | TN +WL | 1 |
| Architekturskizze Informationssystem Gesamtsystem alle vier Firmen (jeweils nur Ausschnitt) | weiss | WL | 1 |
| Rolle des Geschäftsführers (GF) | grün | TN/5 + WL | |
| Informationssicherheitspolitik | grün | TN/5 + WL | 1 |
| Rolle des Informationssicherheitsbeauftragten (ISiBe) | rot | TN/5 + WL | |
| Leitfaden für den Informationssicherheitsbeauftragten (ISiBe) | rot | TN/5 + WL | |
| Sicherheitskonzept TGAG | rot | TN/5 + WL | 1 |
| Rolle des Leiters der Informatik-Abteilung (LInf) | blau | TN/5 + WL | |
| Architekturskizze Informationssystem TGAG (Ausschnitt) | blau | TN/5 + WL | |
| Rolle des Leiters der Revisionsabteilung (LRev) | gelb | TN/5 + WL | |
| Rolle der Benutzer (Ben) | oran-ge | TN/5 + WL | |
| Gesprächsrunden des Workshops | weiss | TN/5 + WL | 1 |

Die Dokumente müssen auf Papier mit der jeweiligen Farbe kopiert werden (rot, gelb, rün, blau, organge, weiss). Ausserdem werden benötigt:

- kleine Papierzettel, welche die Teilnehmer anstecken können (um sie sofort mit einer Rolle zu identifizieren, 1 pro Teilnehmer)
- Sicherheitsnadeln o.ä. zum Anstecken der Papierzettel (1 pro Teilnehmer)
- leere Folien zur Handbeschriftung zur Vorbereitung der Endpräsentationen (3 pro Rolle)
- Folienstifte, am besten wasserlöslich (3 verschiedene Farben pro Rolle)

## 6.3 Architekturskizze Informationssystem Gesamtsystem alle vier Firmen (jeweils nur Ausschnitt)



## 6.4 Rolle des Geschäftsführers (GF)

- Ihre Unternehmung mit 50 Mitarbeitern im Treuhand- und Buchhaltungsbereich macht einen jährlichen Umsatz von mehreren Millionen Franken. Sie sind Geschäftsführer und Mehrheitsaktionär. Sie haben damit *volle* **Verantwortung** für den Gedeih der TGAG und *alle* **Kompetenzen**. Ihr **Ziel** ist eine *florierende, moderne, agile und flexible Unternehmung*.
- Um am Markt bestehen zu können, haben sie immer wieder in neueste Informationstechnologie und in die Ausbildung Ihrer Mitarbeiter investiert. Immer mehr Ihrer Kunden haben E-Mail. Um sie besser und schneller bedienen zu können, haben sie beschlossen, einen Anschluss Ihres Hausnetzes ans Internet in Auftrag zu geben. Sie haben allerdings Angst vor Hackern und möchten deshalb eine Sicherheitsanalyse durchführen. Dazu haben Sie einen Sicherheitsbeauftragten bestimmt, der ein Sicherheitskonzept erarbeiten soll.
- Ihre grösste Angst ist es, dass die Buchhaltung Ihrer Kunden in falsche Hände kommen könnte. Ihre eigene Konkurrenz könnte Ihnen Aufträge abnehmen, die Konkurrenz Ihrer Kunden untereinander könnte sich verschärfen, oder Dritte könnten zu tiefe Einblicke in interne Angelegenheiten Ihrer Kunden erhalten. Sie befürchten ausserdem, dass Ihnen Daten verloren gehen könnten, weil irgend jemand sie löscht. Das würde das Vertrauen Ihrer Kunden in Sie ruinieren, und wäre deshalb geschäftsschädigend.
- Die bei Ihnen verfassten Revisionsberichte werden elektronisch gespeichert und automatisch ausgedruckt und versendet. Wenn sie zwischen Speicherung und Versand verändert werden können, wird Ihre Professionalität angezweifelt.
- Sie möchten nicht, dass Ihre Mitarbeiter frei auf dem Internet surfen, weil sie damit Arbeitszeit verschwenden.
- Sie glauben, dass Revisionsberichte viel schneller beim Kunden sind, wenn Sie diese mit elektronischer Post versenden. Auch für spontane Rückfragen eignet sich E-Mail. Sogar Buchungsbelege oder kleinere Aufträge können Ihre Kunden Ihnen per E-Mail schicken. Ihre eigenen Dienstleistungen und v.a. die Vorteile Ihres Betriebes gegenüber der Konkurrenz möchten Sie im Internet darstellen, weil sie damit Werbekosten sparen.
- Sie sind der Überzeugung, dass Sicherheit nichts kosten darf, denn es handelt sich dabei nur um eine andere Art, die bestehenden Mittel einzusetzen.

**Gespräche**

- Runde 1 (Leitung): Leiten Sie das Gespräch mit dem **Informationssicherheitsbeauftragten [rot]** und dem **Leiter der Revisionsabteilung [gelb].** Teilen Sie ihnen alles über die Ausrichtung des Unternehmens, die Ziele im Markt und bei der Kundschaft, die kritischen Erfolgsfaktoren, und die Nutzeffekte mit, welche Sie sich vom Einsatz von elektronischer Kommunikation und Internet-Anbindung erhoffen. Diskutieren und erstellen Sie die Informationssicherheitspolitik (*IsiPol*) auf Basis der von Ihnen eingebrachten Vorlage.
- Runde 2 (Leitung): Teilen Sie den **Benutzern [orange]** Ihre geschäftlichen Ziele mit und motivieren Sie sie zum sinnvollen Einsatz der Informatik-Mittel. Gewinnen Sie ihre Zustimmung!
- Runde 3: Beobachten Sie den Meinungsaustausch der **Leiter der Informatik [blau]** und **Revision [gelb].** Stellen Sie sich hinter einen der beiden.
- Runde 4 (Leitung): Teilen Sie dem **Leiter der Revision [gelb]** in einem persönlichen Gespräch deutlich mit, was sie von seinen Auffassungen halten und was sie von ihm erwarten.
- Runde 5: Tragen Sie vor, was Sie selbst zur Umsetzung der Informationssicherheit beitragen wollen, wie Sie vorgehen würden und welche Mittel Sie dafür bereitstellen.

## 6.5 Informationssicherheitspolitik

*Ziele und Geltungsbereich*

1.1 Ziel dieser Politik ist der übergreifende und umfassende Schutz aller Informationen der TGAG. Alle in der TGAG vorhandenen Informationen haben einen strategischen Wert. Dies ist unabhängig von Speicherungs- und Übertragungsmedium und betrifft deshalb Dokumente auf Papier ebenso wie auf elektronischen Medien.

1.2 Die Verantwortung für Informationssicherheit muss von allen Personen in der Unternehmung wahrgenommen werden. Jeder Vorgesetzte ist verantwortlich für Umsetzung dieser Politik in seinem Bereich

1.3 ...

## *Grundsätze*

2.1 Wichtigste Ziele der Informationssicherheit sind:

- Wahrung der Verfügbarkeit
- Wahrung der Integrität
- Wahrung der Vertraulichkeit
- Wahrung der Verbindlichkeit

aller eigenen und im Auftrag bearbeiteten Informationen.

2.2 Um die Informationssicherheit zu gewährleisten, müssen Massnahmen ergriffen werden. Diese betreffen alle Bereiche. Die Mitarbeiter müssen den Anweisungen des Informationssicherheitsbeauftragten folgen.

2.3 ...

## *Organisation*

3.1 Für die Gewährleistung der Sicherheit wird ein Informationssicherheitsbeauftragter von der Geschäftsführung bestimmt.

3.2 Aufgaben des ISiBe sind:

- Beratung der Geschäftsführung im Bereich Informationssicherheit und Recht (Datenschutz, Urheberrecht)
- Periodische Berichterstattung an die Geschäftsführung
-

3.3 ...

## *Einzelmassnahmen*

4.1 Mitarbeiter dürfen frei surfen, aber nur 4 Std. pro Woche und alles wird aufgezeichnet und kontrolliert.

4.2 Daten von Kunden dürfen nicht übers Netz übermittelt werden. Alle E-Mails werden deshalb gescannt.

4.3 Datenspeicherung ist nur auf lokalen Geräten erlaubt.

4.4 ...

## 6.6 Rolle des Informationssicherheitsbeauftragten (ISiBe)

- Sie sind der von der Geschäftsleitung der TGAG bestimmte Beauftragte für Informationssicherheit. Es ist Ihre **Aufgabe (Ziel)**, *den Status der Informationssicherheit in der TGAG zu erheben und Vorschläge zur kontinuierlichen und nachhaltigen Verbesserung der Situation zu machen*. Sie haben bisher *keine* **Kompetenzen**, und werden auch *keine* **Weisungsbefugnis** erhalten. Allerdings müssen Sie die Abklärungen innerhalb der Unternehmung vornehmen und der Geschäftsleitung regelmässig Bericht erstatten.
- **Sie sind verantwortlich für die Erstellung des Sicherheitskonzepts.** Die anderen Teilnehmer sind aufgefordert worden, Ihnen dabei zu helfen.
- Halten Sie sich bei der Erarbeitung des Sicherheitskonzepts an den beiliegenden *Leitfaden*. Führen Sie Interviews mit allen beteiligten Personen durch. Notieren Sie sich die wichtigsten Punkte.
- Als Basis für Ihre Arbeit erhalten Sie ein vorgefertigtes *leeres Sicherheitskonzept*. Es steht Ihnen frei, diese Dokumente weiterzuentwickeln, zu ergänzen oder nicht zu beachten. Aufgrund der begrenzten Zeit kann kein vollständiges Konzept entstehen. Versuchen Sie deshalb, *möglichst viele* ***verschiedene*** *Aspekte* zu berücksichtigen.

**Gespräche**

- Runde 1: Erstellen Sie zuerst mit dem **Geschäftsführer [grün]** und dem **Leiter der Informatik-Revision [gelb]** die *Informationssicherheitspolitik (ISiPol)*. Erkundigen Sie sich beim Geschäftsführer nach der Ausrichtung des Unternehmens, den Zielen im Markt, den kritischen Erfolgsfaktoren und den Nutzeffekten, welche er sich vom Einsatz von elektronischer Kommunikation und Internet-Anbindung erhofft. Vom Revisionsleiter erfahren Sie Anforderungen an die Ordnungsmässigkeit der Geschäftsführung und an die Sicherheit des Informationssystems gemäss seiner Untersuchungen in anderen Unternehmungen. Formulieren und verabschieden Sie unter **Leitung des Geschäftsführers** die Politik auf Basis der abgegebenen Vorlage.
- Runde 2 (Leitung): Finden Sie in einem Gespräch mit dem **Leiter der Informatik-Abteilung [blau]** heraus, wie das System aufgebaut ist (eingesetzte Informationssysteme und die wichtigste Informationssammlungen) und welche Schwächen es hat (*Inventur und Risikoanalyse*).
- Runde 3 (Leitung): In einem Gespräch mit den **Benutzern [orange]** identifizieren Sie deren Bedürfnisse und Ängste. Sie müssen die Benutzer und Mitarbeiter motivieren, bei der Umsetzung der Massnahmen zu helfen, und die Sicherheit positiv ins Bewusstsein zu rücken. Halten Sie eine mitreissende Rede, in der Sie die Wichtigkeit der Informationssicherheit betonen.
- Runde 4 (Leitung): Entwickeln Sie mit Hilfe des **Leiters der Informatik [blau]** und den **Benutzern [orange]** einen Massnahmenkatalog, indem Sie Massnahmen definieren, welche die einzelnen Risiken senken.
- Runde 5 (Leitung): Stellen Sie Ihr erarbeitetes Konzept, und die bei der Erstellung gesammelten Erfahrungen vor. Scheuen Sie sich nicht, das (im abgegebenen Leitfaden vorgegebene) Vorgehen zu kritisieren und Verbesserungsvorschläge zu machen. Betonen Sie kritische Erfolgsfaktoren und setzen Sie Prioritäten.

## 6.7 Leitfaden für den Informationssicherheitsbeauftragten (ISiBe)

- Hauptaufgabe des ISiBe ist die Erstellung und Umsetzung eines Sicherheitskonzepts. Dazu müssen Sie verschiedene Gespräche führen, in denen Sie die jeweiligen Ziele der Gesprächspartner herausfinden und die wichtigsten Aussagen notieren. Sie sind selbst Informatiker und haben ein gutes Verständnis von Informationssicherheit. Ihre Gesprächspartner allerdings sind weniger bewandert und haben zum Teil existenzielle Ängste beim Einsatz der Informatik.
- Die Erstellung des Sicherheitskonzepts geschieht (im Workshop) in folgenden Schritten:
  - Erstellung der Informationssicherheitspolitik (ISiPol)
  - Inventur und Wertanalyse der Informatik
  - Bedrohungs- und Risikoanalyse aus Benutzersicht
  - Massnahmenplanung
  - Umsetzungsbeschluss und Umsetzung

**Erstellung der Informationssicherheitspolitik (ISiPol)**

Die Gewährleistung von Informationssicherheit (ISi) ist eine Verantwortung, welche von allen Mitarbeitern getragen werden muss. Damit dies möglich ist, muss der Auftrag zur Betrachtung der ISi von der obersten Führung kommen. Das Top Management wird also - nach einer Sensibilisierung durch Mitarbeiter verschiedener Bereiche - grundlegend festhalten wollen, wie mit Risiken und Sicherheitsproblemen in der Unternehmung umgegangen werden soll. Da dies stark von der Geschäftstätigkeit der Unternehmung abhängt, vom Markt und von weiteren Faktoren, muss die Geschäftsführung in einer Sicherheitspolitik grundlegende Aussagen über die angenommenen Risiken machen.

Es ist Aufgabe des Sicherheitsbeauftragten, die strategische Bedeutung einzelner Informationen und ihres Wertes im geschäftlichen Ablauf zusammenzustellen, Ziele und Richtlinien für den Umgang damit zu formulieren und all dies in einer Sicherheitspolitik der Geschäftsleitung zur Verabschiedung vorzulegen. Ebenfalls müssen gesetzliche und andere Anforderungen (z.B. diejenigen der Revision und des Datenschutzes) berücksichtigt werden.

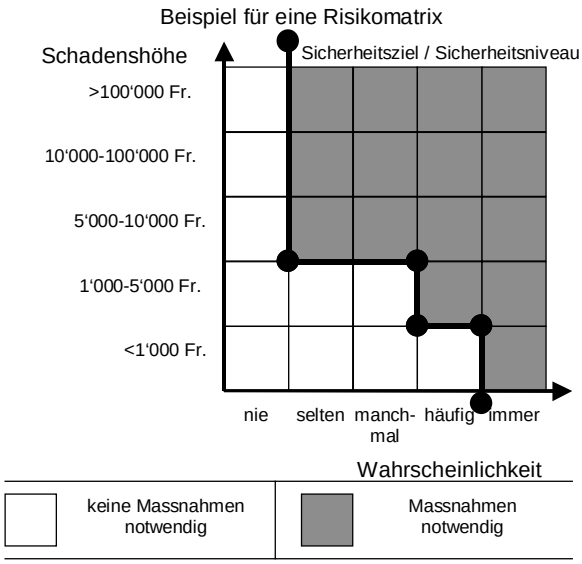
Viele dieser Informationen sind von der Geschäftsführung zu erhalten. Legen Sie diese als allgemeine Ziele, Grundsätze oder organisatorische Elemente fest. Dazu steht Ihnen eine leere Politik zur Verfügung, welche vom Geschäftsführer eingebracht wird. Legen Sie zuerst die Inhalte der Politik fest. Formulieren Sie die einzelnen Elemente dann so um, dass sie Verpflichtungen für einzelne Personen darstellen.

**Inventur und Wertanalyse der Informatik**

Um die Informationssicherheit gewährleisten zu können, müssen Sie zuerst ein Inventar der vorhandenen Informationssammlungen und der Systeme und Prozesse aufstellen, in welchen die Informationen verarbeitet werden. Die dafür erforderlichen Informationen erhält der ISiBe vom Leiter der Informatik und möglicherweise von der Organisationsabteilung, sofern vorhanden. Um Details abzuklären, kann eine Einzelbefragung innerhalb von Abteilungen notwendig sein.

**Bedrohungs- und Risikoanalyse aus Benutzersicht**

- Stellen Sie in einer Grundbedrohungsanalyse fest, welchen Grundbedrohungen (Verlust der Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit) diese einzelnen Informationen ausgesetzt sind.
- Formulieren Sie in einer Bedrohungsanalyse ein Katalog von konkreten Bedrohungen, welche eine der Grundbedrohungen zur Folge haben.
- Halten Sie die erwartete Häufigkeit dieser Bedrohungen fest.
- Schätzen Sie den Schaden ab, welchen der Eintritt einer solchen Bedrohung zur Folge hätte.
- Legen Sie fest, welche dieser Risiken selbst getragen werden sollen, und bei welchen Massnahmen angebracht sind bzw. ergriffen werden sollen. Legen Sie dazu ein Sicherheitsziel fest. Dieser Beschluss muss von der Geschäftsleitung getragen werden. Die Festlegung geschieht am besten mit Hilfe einer Risikomatrix. Die Skalierung der Achsen hängt stark von der Unternehmung ab und muss durch Diskussion bestimmt werden.




**Massnahmenplanung**

Sobald festgelegt ist, welche Risiken nicht getragen werden sollen, müssen Massnahmen formuliert werden, welche diese Risiken senken. Das geschieht individuell pro bedrohtem Objekt (Informationssammlung, Prozess, Gerät, etc.). Einzelne Objekte können mit mehreren Massnahmen geschützt werden; einzelne Massnahmen können aber auch mehrere Objekte schützen. Alle Massnahmen werden in einem Katalog zusammengestellt, wobei idealerweise pro Massnahmen Kosten und Nutzen ausgewiesen werden.

**Umsetzungsbeschluss und Umsetzung**

Die Umsetzung der Massnahmen wird den betroffenen Stellen vorgeschlagen, welche sich für oder gegen die Umsetzung entscheiden und diese selbst durchführen (i.d.R. keine Weisungsbefugnis des ISiBe). Diese Entscheidungen müssen dokumentiert werden. Die nicht durch Massnahmen gesenkten Risiken stellen Restrisiken dar, über welche die Geschäftsführung informiert werden muss.

Die Massnahmen aus dem Katalog müssen in der Folge umgesetzt werden, wobei der ISiBe eine Kontrollfunktion hat: er muss periodisch über die Einhaltung und Umsetzung der Politik und der beschlossenen Massnahmen an die Geschäftsleitung berichten. Periodisch oder bei grösseren Veränderungen der Informationssysteme muss er in Zusammenarbeit mit den betroffenen Stellen diesen Ablauf erneut durchführen.

## 6.8 Sicherheitskonzept TGAG

# Sicherheitspolitik

Wichtigste Inhalte der Sicherheitspolitik sind:

- ...

# Inventar

| Nr | Objektname | Beschreibung | Verantwortlicher | Wert (Fr.) |
|---|---|---|---|---|
| I01 | | | | |
| I02 | | | | |
| I03 | | | | |
| I04 | | | | |
| I05 | | | | |
| I06 | | | | |
| I07 | | | | |
| I08 | | | | |
| I09 | | | | |
| I10 | | | | |

Hinweise:

- Erheben Sie aufgrund der Architekturskizze Objekte der Kategorien Hardware, Software, Papier, Datensammlungen, Infrastruktur (Netze, Strom, etc.), Kommunikation, Personen. Konzentrieren Sie sich auf ein paar wesentliche, unterschiedliche Objekte!
- Als Wert können Sie Neuwert (N), Wiederbeschaffungswert (W), Zeitwert (Z), oder internen Wert (I) verwenden.

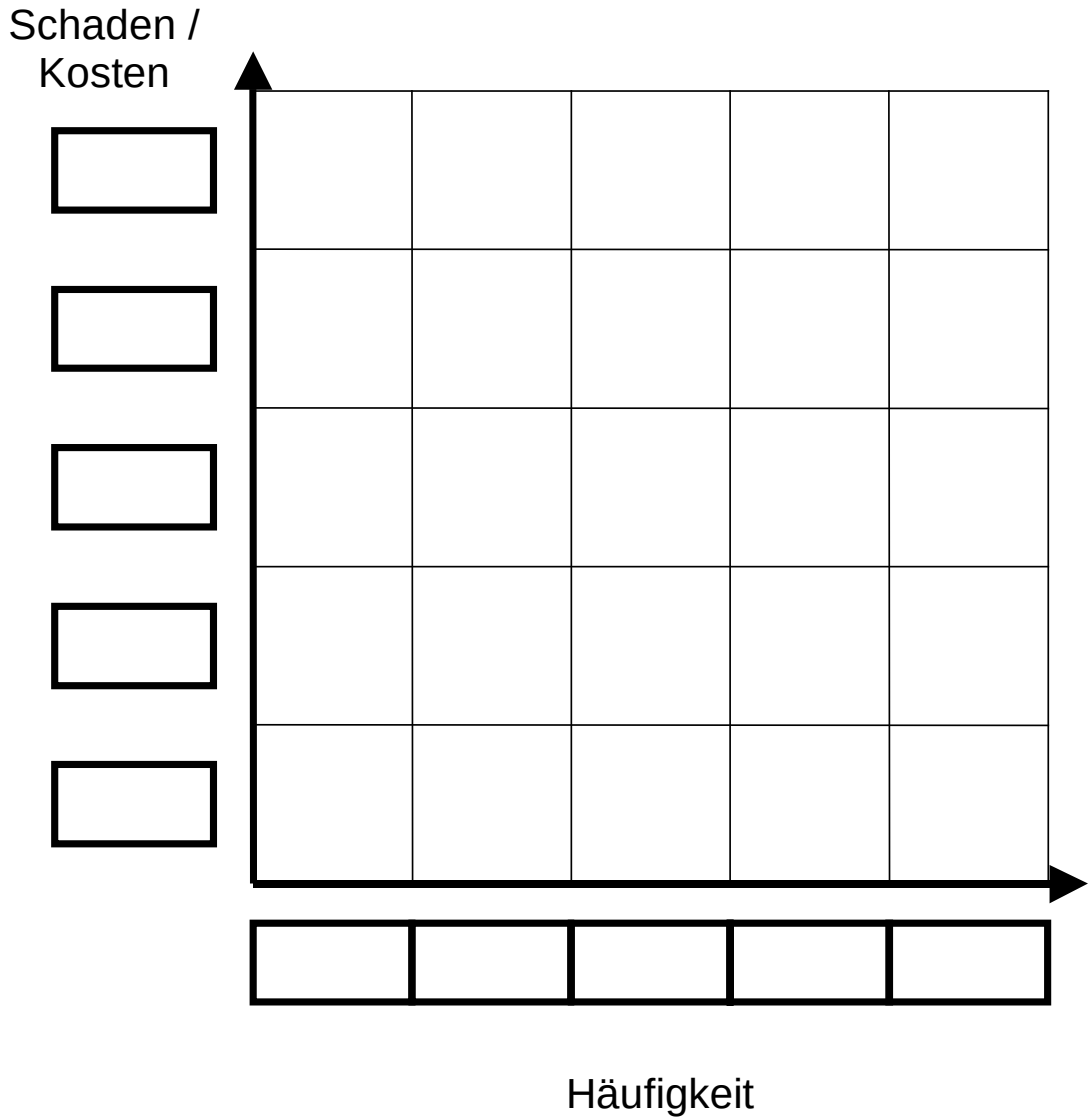
# Bedrohungen

| Nr. | Name | Szenario | Betroffene Objekte | Folgebedrohungen |
|---|---|---|---|---|
| B01 | | | | |
| B02 | | | | |
| B03 | | | | |
| B04 | | | | |
| B05 | | | | |
| B06 | | | | |
| B07 | | | | |
| B08 | | | | |
| B09 | | | | |
| B10 | | | | |
| B11 | | | | |
| B12 | | | | |

# Risiken

| Nr. | Bedrohungen | Beschreibung | Häufigkeit | Kosten | Feld |
|---|---|---|---|---|---|
| R01 | | | | | |
| R02 | | | | | |
| R03 | | | | | |
| R04 | | | | | |
| R05 | | | | | |
| R06 | | | | | |
| R07 | | | | | |
| R08 | | | | | |
| R09 | | | | | |
| R10 | | | | | |
| R11 | | | | | |
| R12 | | | | | |

## Risikomatrix



# Massnahmen

| Nr. | Beschreibung | gesenkte Risiken | Kosten | Verantwortlicher | Termin |
|---|---|---|---|---|---|
| M01 | | | | | |
| M02 | | | | | |
| M03 | | | | | |
| M04 | | | | | |
| M05 | | | | | |
| M06 | | | | | |
| M07 | | | | | |
| M08 | | | | | |
| M09 | | | | | |
| M10 | | | | | |
| M11 | | | | | |

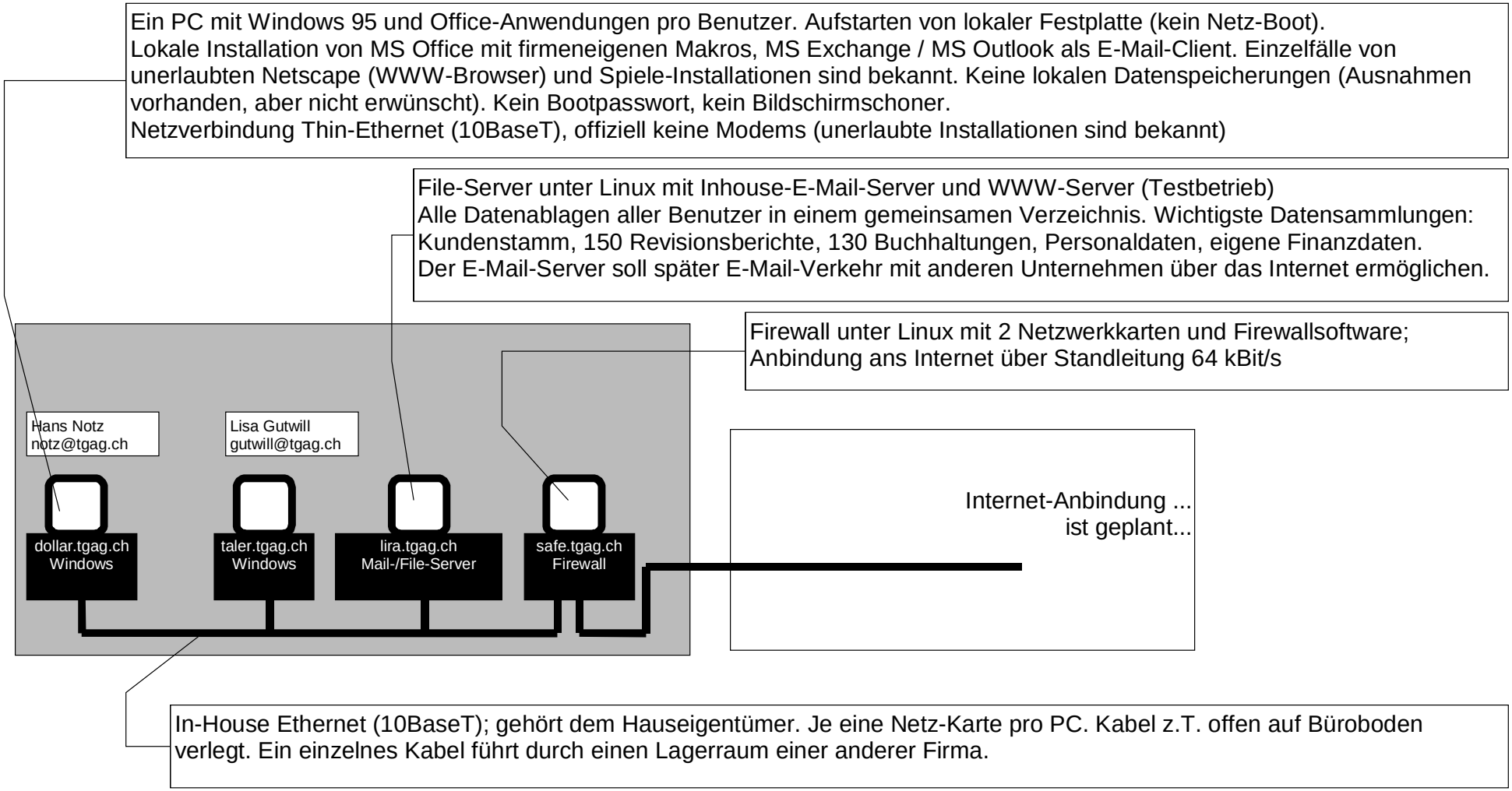
## 6.9 Rolle des Leiters der Informatik-Abteilung (LInf)

- Sie sind der Leiter der Informatik-Abteilung, welche das gesamte Informatik-System der TGAG betreut. Sie sind **verantwortlich** für *Funktion und Sicherheit des Systems*, besprechen notwendige und gewünschte Systemausbauten mehrmals jährlich mit dem Geschäftsführer und *verfügen über ein bewilligtes Budget (***Kompetenz***)*. Ihr **Ziel** ist ein *effizienter Mitteleinsatz und eine gute Unterstützung der Geschäftstätigkeit durch Informatik*.
- Das System ist folgendermassen aufgebaut (vgl. auch Architektur-Skizze):
  - Jeder Benutzer hat ein persönliches Gerät (PC) mit Windows, Office-Applikationen und E-Mail-Programm. Internet-Anwendungen sind bisher nicht installiert.
  - Jeder PC startet von seinem Harddisk, und alle Programme sind dort installiert. Alle Daten müssen auf einem File-Server gespeichert werden (Netzlaufwerk). Jeder Benutzer muss sich am System mit Name und Passwort anmelden, um darauf zugreifen zu können. Daten auf lokalen Geräten werden nicht gesichert.
  - Der Server läuft unter Linux (ein UNIX-Derivat) und bietet ein E-Mail-Postbüro und (versuchsweise) einen WWW-Server.
- Sie haben einige Sorgen:
  - In letzter Zeit haben Sie zweimal erlebt, dass Mitarbeiter ein Modem an Ihren PC angeschlossen haben, um sich ins Internet einzuwählen.
  - Bildschirmschoner haben sie keine installiert, weil einige Mitarbeiter den PC aus- und wieder einschalten, wenn der Bildschirm dunkel ist.
  - Ihre Büros sind im dritten Stock eines Gewerbegebäudes. Der Betrieb im Stockwerk unter Ihnen hat um fünf Uhr morgens Arbeitsbeginn, empfängt viele Besucher und lässt die Eingangstüren oft offen stehen. In Ihrem Stockwerk hat er ein Lager, durch welches Ihre Netzwerkkabel laufen.
  - Manchmal haben sie Stromstörungen, wenn unter Ihnen Maschinen ein- und ausgeschaltet werden, welche oft zum Absturz mehrerer Geräte führen. Sie haben schon mehrfach Geld für einen Stromfilter und eine Notstromversorgung verlangt, aber die Geschäftsleitung will davon nichts wissen.
- Helfen Sie dem Informationssicherheitsbeauftragten bei der Erstellung des Sicherheitskonzepts.

**Gespräche**

- Runde 1 (Leitung): Erläutern Sie den **Benutzern [orange]** das Informationssystem und erfragen Sie Befürchtungen und Anforderungen, gerade im Hinblick auf die bevorstehende Internet-Anbindung.
- Runde 2: Der **Informationssicherheitsbeauftragte [rot]** möchte von Ihnen den genauen Aufbau Ihrer Informatik-Installation wissen, um *Inventur und Risikoanalyse* durchzuführen. Geben Sie Ihm die beigelegte Architekturskizze und erläutern Sie sie aufgrund der oben angegebenen Informationen.
- Runde 3 (Leitung): Sie schneiden bei der Informatik-Revision durch eine befreundete externe Revisionsfirma immer recht gut ab. Fragen Sie den **Leiter der Revisionsabteilung [gelb]** ein bisschen über seine Vorgehensweise aus, wenn er andere Firmen revidiert. Erzählen Sie ihm anschliessend Ihre eigenen Auffassungen. (wird vom **Geschäftsführer [grün]** beobachtet)
- Runde 4: Helfen Sie dem **Informationssicherheitsbeauftragten [rot]** in Zusammenarbeit mit den Benutzern eine Massnahmenliste zu erstellen.
- Runde 5: Stellen Sie die sinnvollsten und wichtigsten Massnahmen und ihre Auswirkungen auf Betrieb des Systems und die Informatik-Kosten vor.

## 6.10 Architekturskizze Informationssystem TGAG (Ausschnitt)



## 6.11 Rolle des Leiters der Revisionsabteilung (LRev)

- Sie sind der Leiter der Revisionsabteilung, welche mehr als die Hälfte des Umsatzes der TGAG erwirtschaftet. Ihr **Ziel** ist *weiteres langsames Wachstum der Abteilung*. Sie sind für die *sorgfältige Abwicklung von Fremdrevisionen* **verantwortlich** und *haben die dazu notwendigen* **Kompetenzen** *in Ihrer Abteilung*.
- Aufgrund Ihrer regelmässigen Lektüre des „Schweizer Revisor“ und ihrer Erfahrungen bei der Revision Ihrer Mandanten halten Sie überhaupt nichts von einer Internet-Anbindung. Das würde Ihren Mitarbeitern erlauben, alle internen Informationen einfach irgendwo hin zu schicken und öffnet Hackern Tür und Tor.
- Sie sind inzwischen überzeugt, dass Computer Ihnen bei Ihrer Arbeit helfen, aber E-Mail benutzen Sie auch intern nicht, weil sie eine Grenze zwischen TGAG und Aussenwelt ziehen wollen. Die TGAG ist schliesslich eine selbständige Unternehmung und muss sich nicht zu tief in Ihre Karten blicken lassen.
- Die Informatik-Mittel, die sie benutzen, werden von der Informatik-Abteilung betreut, welche auch für die Sicherheit zuständig ist und bei Problemen technischen Support bieten muss. Sie selbst beschränken sich auf die Speicherung Ihrer Revisionsberichte und der dazu notwendigen Datenbanken und auf die elektronische Verwaltung Ihrer Briefmarkensammlung. Bisher gab es noch keine Sicherheitsvorfälle. Nur einmal haben Sie mehrere Berichte neu anfertigen müssen, weil die Informatik-Abteilung keine Kopie von den Daten auf der Festplatte Ihres persönlichen PCs angelegt hatte. Den Inhalt dieser Festplatte dürfen die Informatiker auch nicht sehen, aber dass sie ihn nicht wiederherstellen konnten, zeugt von der Unfähigkeit der Informatik-Abteilung. Alle Daten irgendwo im Netz zu speichern halten Sie für Unsinn, weil sie glauben, dass Sie die Daten nicht wiederfinden können und dass dann jeder darauf zugreifen kann. Ausserdem wird das Netz durch die Internet-Anbindung weltweit.
- Sie verwenden einen gemeinsamen Drucker mit Ihren drei Nachbarbüros, der an Ihrem PC angeschlossen ist. Dazu hat man Ihnen „Datei- und Druckerfreigabe“ eingeschaltet.
- Um einen Einblick ins Internet zu gewinnen, haben Sie bei Ihrem besten Kollegen im Nachbarbüro ein bisschen „gesurft“. Sein Sohn war dagewesen, hatte ein Modem an Büro-PC und Telefon seines Vaters angeschlossen und die notwendigen Programme eingerichtet.
- Die interne Informatik der TGAG wird nicht von Ihnen revidiert, sondern von einer befreundeten Revisionsgesellschaft. Diese stellt der TGAG und ihren Informatikern immer gute Zeugnisse aus, nur Ihrer eigenen (Revisions-) Abteilung nicht. Das verstehen sie nicht.
- Helfen Sie dem Informationssicherheitsbeauftragten bei der Erstellung des Sicherheitskonzepts.

**Gespräche:**

- Runde 1: Helfen Sie dem **Geschäftsführer [grün]** und dem **Informationssicherheitsbeauftragten [rot]** dabei, die Ziele der Informationssicherheit in einer *Politik* zu formulieren. Lassen Sie ihre eigenen Auffassungen einfliessen, aber der Geschäftsführer hat das letzte Wort.
- Runde 2: Beobachten Sie das Gespräch zwischen **Geschäftsführer [grün]** und **Benutzern [braun].** Lassen auch sie sich motivieren, aber zweifeln sie einzelne Argumente des Geschäftsführers öffentlich an.
- Runde 3: Um herauszufinden, was hinter der guten Benotung der Informatik-Abteilung steckt, unterhalten Sie sich mit deren **Leiter [blau]**. Sie fragen ihn nach seiner eigenen Vorstellung von Sicherheit und seiner Meinung zum Internetanschluss. Im Anschluss daran teilen Sie ihm Ihre eigenen Anforderungen an die Sicherheit mit.
- Runde 4: In einem persönlichen Gespräch teilt Ihnen der **Geschäftsführer [grün]** seine Auffassung von Informatikmittel-Einsatz und Informationssicherheit mit. Halten Sie dagegen!
- Runde 5: Erläutern Sie Ihre Ansichten, Ihre Erfahrungen und Ihre Bedenken und die Rolle, welche Sie bei der Umsetzung der Sicherheitsmassnahmen spielen möchten.

## 6.12 Rolle der Benutzer (Ben)

- Sie sind einer der 50 Mitarbeiter der TGAG, erfüllen Ihre Aufgaben innerhalb der Revisions- oder Buchhaltungsabteilung, und haben *wenig* **Verantwortung** oder **Kompetenzen**.
- Für Ihre Arbeit steht Ihnen ein PC zur Verfügung, der von der Informatik-Abteilung gewartet wird. Die Arbeit wird immer schwieriger, weil es immer mehr zu beachten gibt, und Ihre Partner bei den Mandanten immer schneller über alles informiert werden wollen. Oft sind diese jedoch telefonisch nicht zu erreichen, so dass sich Ihre Arbeit verzögert.
- Vielfach erhalten Sie Dokumente, welche Ihre Mandanten bei sich im Computer gespeichert und dann ausgedruckt haben. Diese müssen Sie dann neu eintippen, weil Sie sie auf Papier ausgedruckt in der Post bekommen haben.
- Ihre Textverarbeitung ist irgendwie anders als bei Ihrer vorherigen Arbeitsstelle eingerichtet. Oft genügt ein Tastendruck, um komplizierte Formulierungen einzufügen. Auch Ihre Finanzbuchhaltungsdaten können Sie mit der Textverarbeitung formatieren.
- Sie machen sich Sorgen, ob jemand etwas von den Spielen bemerkt, die sie heimlich installiert haben und nach Feierabend spielen. Ihr PC musste schon mehrmals neu eingerichtet werden, nachdem Sie einen „Virus“ hatten.
- Letzthin hat Sie ein Mandant überraschend in Ihrem Büro besucht, während Sie die Daten eines anderen Mandanten bearbeiteten. Als er mal kurz telefonieren wollte, haben Sie ihn in Ihrem Büro alleine gelassen.
- Ihre Kollegin, die bei einer anderen Treuhandgesellschaft arbeitet, bekommt Provisionen für jeden neu geworbenen Mandanten. Deshalb drucken Sie die Mandantenliste Ihrer eigenen Firma aus und geben Sie Ihrer Freundin, um ihr bei ihrer Arbeit zu helfen. Später wollen Sie von der gewonnenen Provision gut zum Essen ausgehen.
- Sie möchten auch mal „surfen“. Ein Kollege hat ein Modem in seinem Büro und sie haben mal einen Abend lang Spiele heruntergeladen und dann gespielt. Einer Ihrer Kollegen hat ein paar CDs über das Internet bestellt und zur Abrechnung seine Kreditkartennummer angegeben.

**Gespräche:**

- Vorbemerkung: Entscheiden Sie sich, ob sie die Rolle eines geschäftlich motivierten, engagierten Benutzers spielen wollen, diejenige eines Power-Users (v.a. technisch motiviert) oder diejenige eines unmotivierten, möglicherweise frustrierten Mitarbeiters. Überlegen Sie, wie alt die Person ist, die sie spielen wollen.
- Runde 1: Erläutern Sie Ihre Wünsche und Ängste dem **Leiter der Informatik-Abteilung [blau]**. Stellen Sie sich stur, wenn er Ihnen das Surfen über selbst installierte Modems und die Installation von Spielen untersagen will, weil das „Ihre einzige Freude am Arbeitsplatz“ sei.
- Runde 2: In einem Vortrag informiert Sie der **Geschäftsführer [grün]** über Sinn und Zweck des Informatik-Einsatzes, bevorstehende Erweiterungen des Systems und appelliert an Ihr sicheres und verantwortungsvolles Verhalten. Lassen Sie sich in Ihrer Arbeit nicht einschränken und diskutieren Sie über Sinn und Zweck der Internet-Anbindung.
- Runde 3: Der **Informationssicherheitsbeauftragte [rot]** befragt Sie über die Informationen, die sie verwenden. Sagen Sie ihm, sie hätten Buchhaltungsdaten, eine Mandantenliste, Revisionsberichte, Zeiterfassungsberichte und Rechnungen an Mandanten. Schildern Sie ihm Ihre Bedürfnisse und Ängste.
- Runde 4: Helfen Sie dem **Informationssicherheitsbeauftragten [rot]** und dem **Leiter der Informatik [blau]** bei der Formulierung sinnvoller Sicherheits-Massnahmen.
- Runde 5: Stellen Sie Ihre eigenen Erfahrungen und Ängste vor, sowie das Potential der Internet-Anbindung, wie sie es sehen.

## 6.13 Gesprächsrunden des Workshops

| Start | Ende | Run-de | Aufgabe | Teilnehmer | Ort |
|---|---|---|---|---|---|
| 8:15 | 8:30 | | Einführung und Ablauf | Workshop-Leiter | |
| 8:30 | 8:45 | 0 | Verteilen und Lesen der Rollen | | |
| 8:45 | 9:15 | 1a | Erstellung der ISiPol | GF (Leitung), ISiBe, LRev | |
| 8:45 | 9:15 | 1b | Anforderungsanalyse | LInf (Leitung), Ben | |
| 9:15 | 9:45 | 2a | Inventur und Wertanalyse | ISiBe (Leitung), LInf | |
| 9:15 | 9:45 | 2b | Awareness | GF (Leitung), Ben, LRev | |
| 9:45 | 10:15 | | Kaffeepause | alle | |
| 10:15 | 10:45 | 3a | Bedrohungs- und Risikoanalyse | ISiBe (Leitung), Ben | |
| 10:15 | 10:45 | 3b | Erfahrungsaustausch (Erfa) | LInf (Leitung), LRev, GF | |
| 10:45 | 11:15 | 4a | Erstellung Massnahmenkatalog | ISiBe (Leitung), LInf, Ben | |
| 10:45 | 11:15 | 4b | Korrektur ISi-Auffassung | GF (Leitung), LRev | |
| 11:15 | 11:30 | | Pause | alle | |
| 11:30 | 12:00 | 5 | Koordination der Vorträge | jeweils alle pro Rolle | |
| 12:00 | 12:45 | 5 | Vorstellung erarbeitetes Sicher-heitskonzept und Erfahrungen | Ben (15 Min.)<br>LRev (15 Min.)<br>LInf (15 Min.) | |
| 12:45 | 13:00 | | Pause | | |
| 13:00 | 13:30 | 5 | Vorstellung erarbeitetes Sicher-heitskonzept und Erfahrungen | ISiBe (15 Min.)<br>GF (15 Min.) | |
| 13:30 | 13:40 | 6 | Diskussion und Abschluss | alle | |

# Rollen und Farben

| Rolle | Abkürzung | Farbe |
|---|---|---|
| Informationssicherheitsbeauftragter | ISiBe | [rot] |
| Geschäftsführer | GF | [grün] |
| Leiter der Revision | LRev | [gelb] |
| Leiter der Informatik | LInf | [blau] |
| Benutzer | Ben | [orange] |
| Allgemein / Workshop-Leitung / Moderation | | [weiss] |

