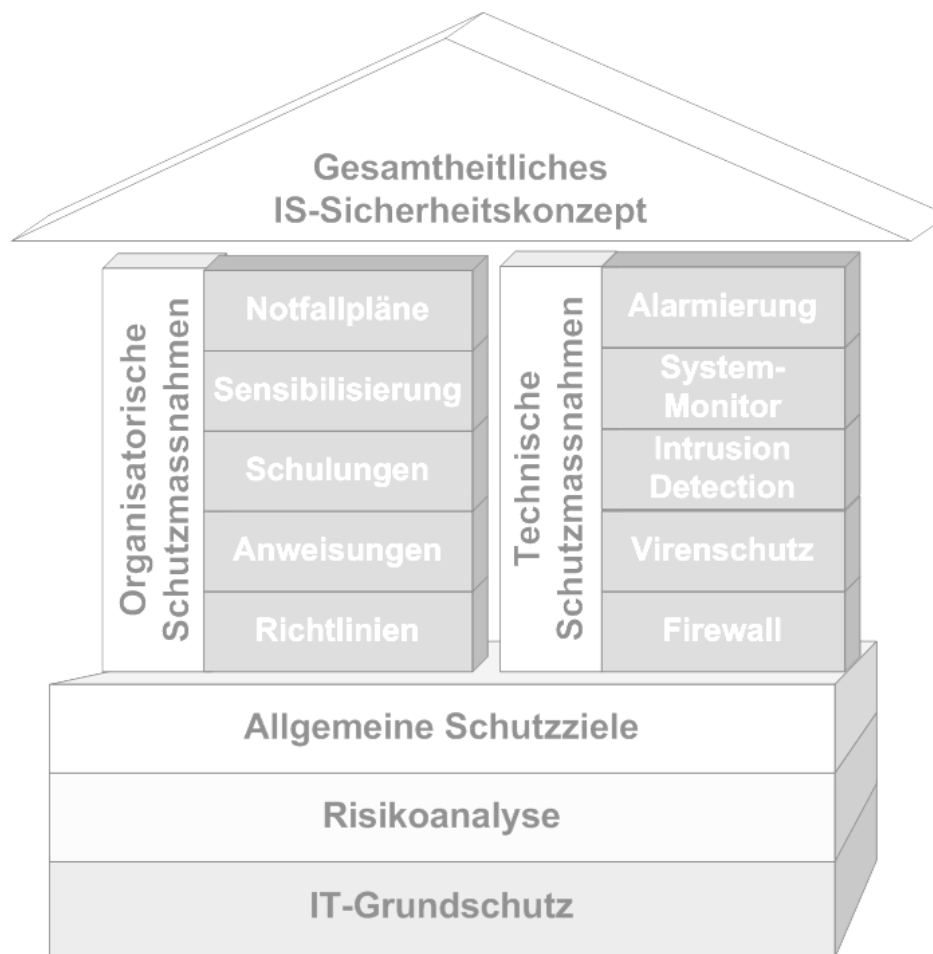


# „Informationssicherheit“



## eine ganzheitliche Aufgabe

## Inhaltsverzeichnis

<b>1. Einleitung .....</b>	<b>3</b>
1.1 Vorgehen und Methode .....	3
1.1.1 IS-Sicherheitspolitik .....	3
1.1.2 Informationssicherheits-Managementprozess .....	4
1.1.3 Hohe Service Standards - auf fundierter Basis .....	5
1.1.4 Modul für Modul zur umfassenden Sicherheit .....	6
<b>2 Basis-Services .....</b>	<b>8</b>
2.1 Basisanalyse: Ihre IT-Security im Visier .....	9
2.2 Kundenforum: Informatiksicherheit für Entscheider .....	10
<b>3 Weiterführende Services .....</b>	<b>11</b>
3.1 Detailanalysen .....	12
3.1.1 Benchmark-Analyse: Ihre Sicherheitsziele auf dem Prüfstand .....	12
3.1.2 Control Self Assessment (CSA): Sehen Sie die Sicherheit Ihres Unternehmens mit anderen Augen .....	13
3.1.3 Impact Analysis: Der Sicherheitsspielraum Ihrer IT .....	14
3.1.4 Machbarkeitsstudie: Frühzeitige Analysen zur Risikominimierung .....	15
3.1.5 Penetration Test: Mehr Sicherheit durch „simulierte“ Attacken .....	16
3.1.6 Risikoanalyse: Der gezielte Gefahrencheck .....	17
3.1.7 SAP-Security: Komplexe Anforderungen, präzise Lösungen .....	18
3.2 IS-Sicherheitskonzept: Sicherheit in allen Unternehmensbereichen .....	19
3.2.1 Ausgangspunkt: „Informatiksicherheit“ – eine ganzheitliche Aufgabe .....	19
3.2.2 Die richtige Basis: Ein ausgefeiltes Sicherheitskonzept .....	19
3.2.3 Schritt für Schritt zum umfassenden Sicherheitskonzept .....	20
<b>4 Periodische Services .....</b>	<b>21</b>
4.1 Periodisches Audit: Kontinuierliche Sicherheit im dynamischen IT-Umfeld .....	22
<b>5 Begleitende Services .....</b>	<b>23</b>
5.1 Schulungen/Workshops: Fundiertes Know-how für alle Bereiche .....	24
5.2 Pflichtenheft / Evaluation: Das Komplettangebot rund um das Einholen von Angeboten .....	25

## 1. Einleitung

In den meisten Unternehmungen ist die Informatik ein nicht mehr wegzudenkendes Hilfsmittel geworden. Es stellt sich zunehmend die Frage, wie Unternehmungen die ständige Herausforderung, ihre Informatikmittel und Daten vor Hackern, Viren, Diebstahl, Fälschungen oder Schäden durch physikalische Einwirkungen wie Feuer, Wasser oder Erdbeben zu schützen vermögen. Die Aufgabe der Gewährleistung der Informatiksicherheit in einem Unternehmen ist deshalb eine sehr aufwändige Aufgabe geworden. Sie besteht nicht mehr nur aus einer rein technischen Betrachtungsweise auf eine Unternehmung, sondern viele verschiedene Einflussfaktoren wie die Organisationsstrukturen, das Verhalten der Mitarbeiter, dediziertes Know-how Einzelner etc. beeinflussen zunehmend die Informationssicherheit einer Unternehmung. Daher spielen Informationssysteme und ihr Schutz eine immer wichtigere Rolle und tragen entscheidend zur Wettbewerbsfähigkeit und somit zum Unternehmenserfolg bei. Meist ist zwar der direkte Nutzen von Sicherheitsmassnahmen nicht unmittelbar ersichtlich, doch Lücken im System können grossen Schaden anrichten. Zudem bestehen heute gesetzliche Regelungen (DGB, OR, etc.), die den Entscheidern einer Unternehmung die Verantwortung für die Informationssicherheit zuweisen und die Verantwortlichen auch zur Rechenschaft ziehen. Dies alles spricht für eine erhöhte Aufmerksamkeit für ein integriertes IS-Sicherheitskonzept<sup>1</sup> in jeder Unternehmung.

### 1.1 Vorgehen und Methode

uniQconsulting ag hat aus ihrer langjährigen Erfahrung im IS-Sicherheitsumfeld eine Methodik entwickelt, mit Hilfe dieser die anstehenden Arbeiten optimal unterstützt werden. Diese Methodik umfasst die IS-Sicherheitspolitik als normatives Element, den Informationssicherheits-Managementprozess sowie das IS-Sicherheitskonzept, das sich aus mehreren Modulen zusammensetzt. Diese Module umfassen alle kritischen Unternehmensbereiche und werden entlang des Informatiksicherheits-Managementprozesses implementiert. Im Folgenden wird das von uniQconsulting entwickelte IS-Sicherheitskonzept vorgestellt.

#### 1.1.1 IS-Sicherheitspolitik

Die Grundlage des IS-Sicherheitskonzepts bildet die IS-Sicherheitspolitik. Die IS-Sicherheitspolitik wird definiert durch die Geschäftsleitung und beschreibt die Ziele, die durch die Informationssicherheit erreicht werden sollen. Dabei werden die Ziele für alle Bereiche einer Unternehmung bestimmt und können gemäss der Struktur in Abbildung 1 genauer runter gebrochen werden. Die IS-Sicherheitspolitik sollte wie alle Unternehmensziele in regelmässigen Abständen überprüft und bei Bedarf angepasst werden. Die IS-Sicherheitspolitik ist der normative Ausgangspunkt im Informationssicherheits-Managementprozess der für ein ganzheitliches IS-Sicherheitskonzept durchschritten werden sollte.

---

<sup>1</sup> IS steht für Information Systems

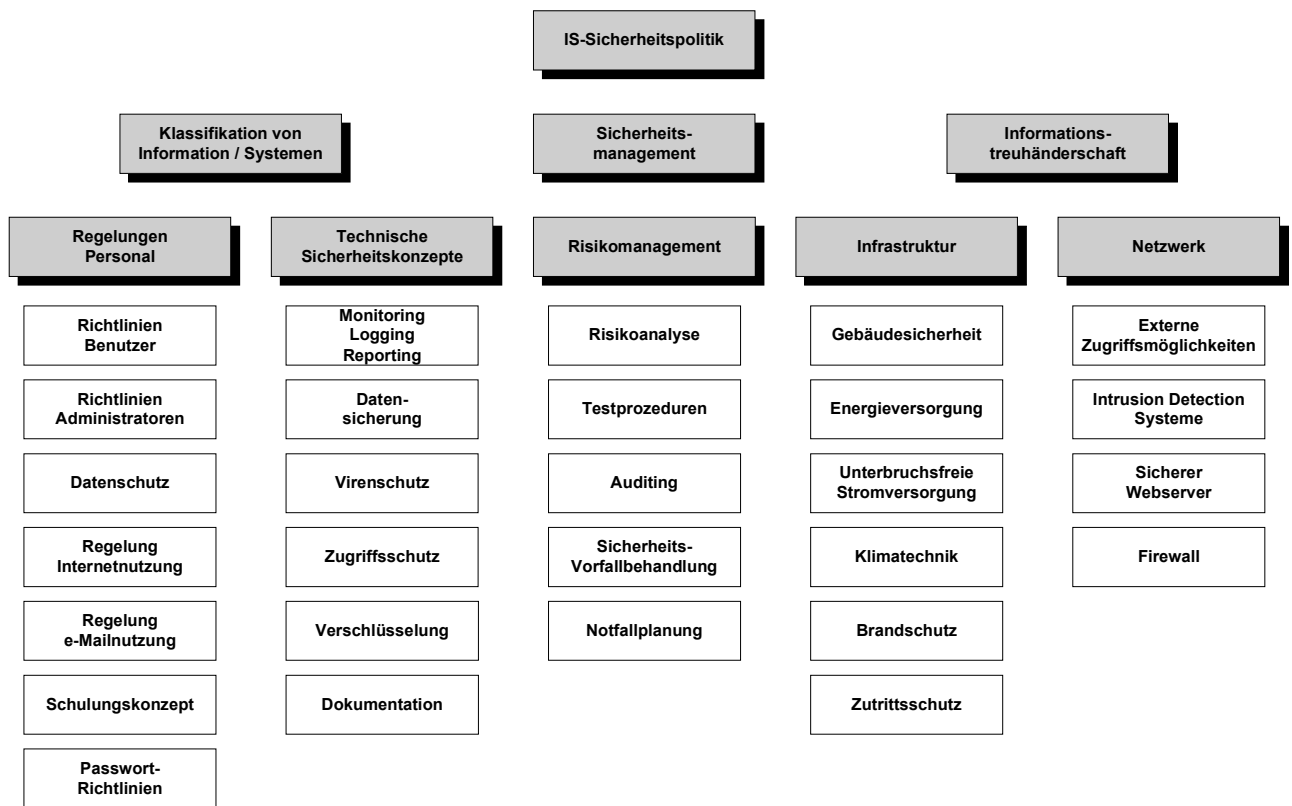


Abbildung 1: Struktur des IS-Sicherheitskonzepts

## 1.1.2 Informationssicherheits-Managementprozess

Nach erfolgter IST-Aufnahme der Sicherheitsziele werden entlang dem nachfolgend dargestellten Informationssicherheits-Managementprozess in Abbildung 2 die fehlenden oder unvollständigen Bestandteile identifiziert und der notwendige Handlungsbedarf ermittelt. Dabei gilt es zu berücksichtigen, dass gegebenenfalls im Bereich der Sicherheitsziele Anpassungen erforderlich sind.

In Abbildung 2: Informationssicherheits-Managementprozess muss deutlich unterschieden werden zwischen den reinen Analyse- und definitorischen Tätigkeiten (siehe Markierung) und der Umsetzung der abgeleiteten Massnahmen. Dabei ist zu berücksichtigen, dass aus formalen Gründen die definitorisch-analytischen Module nicht von ein und derselben Institution durchgeführt werden sollten, da etwaige Konflikte bei der Umsetzung möglich sein könnten.

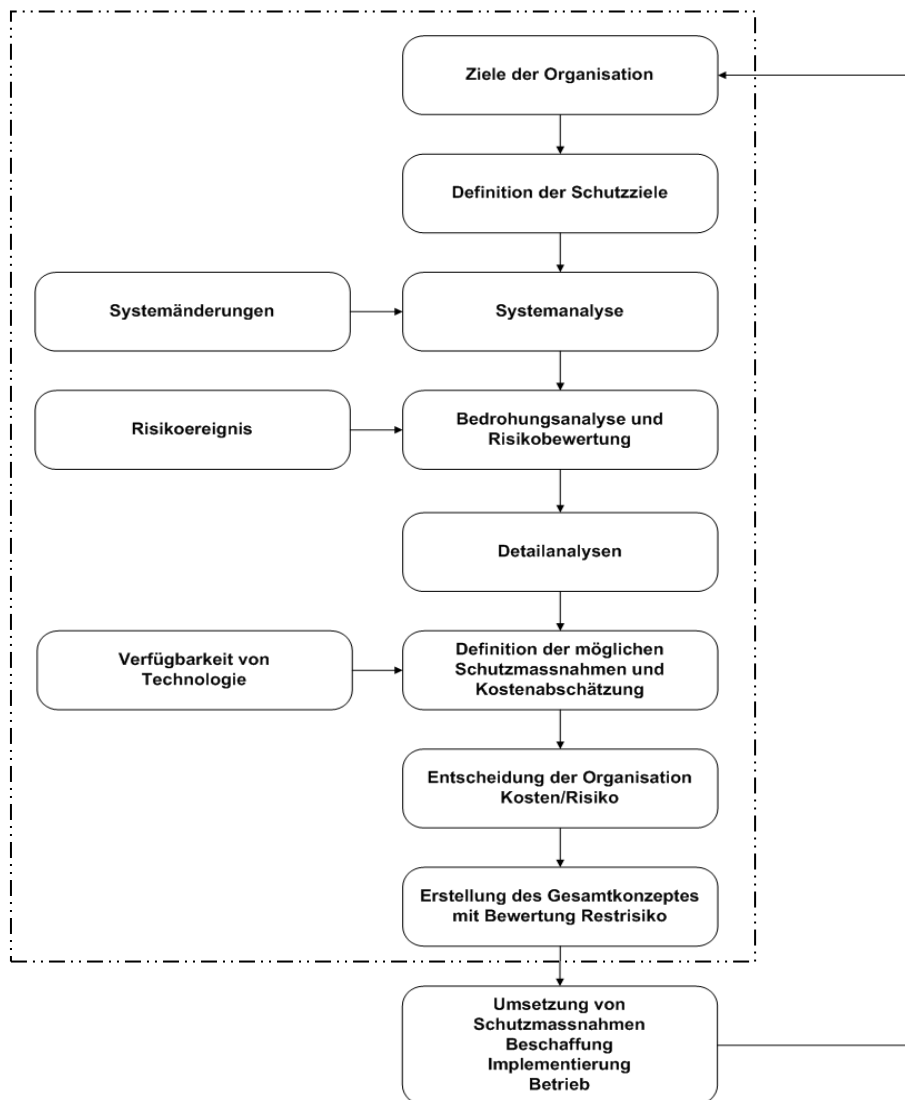


Abbildung 2: Informationssicherheits-Managementprozess

### 1.1.3 Hohe Service Standards - auf fundierter Basis

uniQconsulting bietet ganzheitliche Systeme für umfassende Informatiksicherheit, von der ersten Risikoanalyse über das massgeschneiderte Sicherheitskonzept bis hin zum prozessbegleitenden Controlling. Projektbezogen greifen wir bei Bedarf auf weitere kompetente Partnerunternehmen zurück. Insbesondere bei den technischen Schutzmassnahmen und dem Einsatz spezifischer Produkte (z.B. Firewalls, IDS, Secure E-Mail, Virenschutz o.Ä.).

Aus unserer Projekterfahrung ist mittlerweile ein umfangreiches, sich ergänzendes Produktportfolio entstanden. Dieses Portfolio fokussiert auf die erfolgreiche, qualifizierte Zertifizierung der Informatiksicherheit unserer Kunden. Nachfolgend eine Übersicht des gesamten Portfolios:

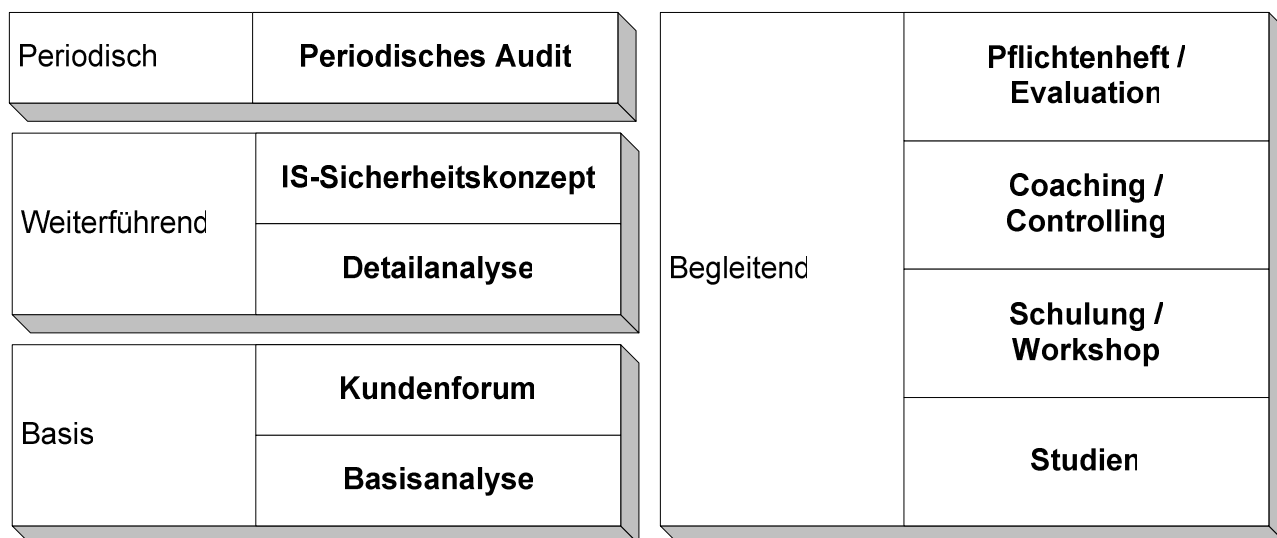


Abbildung 3: IS-Service Portfolio

#### 1.1.4 Modul für Modul zur umfassenden Sicherheit

Die einzelnen Module unseres Portfolios ergänzen sich zu einem sinnvollen Ganzen, das alle kritischen Bereiche abdeckt: von Self-Assessments, Sicherheits-Audits und –Berichten über Risikoanalysen und Sicherheitskonzepte bis hin zu Controlling- und Coaching-Dienstleistungen.

Dieser „Grundschutz“ wird anhand einer Gefährdungsanalyse, den allgemeinen Schutzziele und den spezifischen Bedürfnissen der Organisation erweitert. Diese Erkenntnisse bilden nun die Grundlage zur Erstellung von Richtlinien aus welchen sich die organisatorischen und technischen Massnahmen ableiten lassen.

Jede, auch noch so kleine Schwachstelle gefährdet das gesamte Sicherheits-System. Daher konzentrieren wir uns – im Gegensatz zu vielen unserer Mitbewerber - nicht nur auf die rein technischen Aspekte, sondern berücksichtigen alle relevanten organisatorischen und rechtlichen Gesichtspunkte. Anders gesagt: Unsere Spezialisten entwickeln individuelle Lösungen, die umfassende Informatiksicherheit garantieren.

Um die Sicherheit von IS-Systemen gewährleisten zu können, sind ausgewogene Schutzmassnahmen notwendig. Dafür sind Massnahmen in den organisatorischen Bereichen und der Einsatz von technischen Mitteln notwendig.

In erster Linie sind die Massnahmen aus beschriebenen und teilweise frei erhältlichen „Baselines“ abzuleiten. Bei den „Baselines“ handelt es sich um von unterschiedlichen Organisationen beschriebene Methoden zur Analyse, Aufbau und Implementierung von Sicherheitsrichtlinien.

Alle Informatik-Sicherheitsanalysen basieren auf anerkannten Standards wie:

- Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik (BSI)  
[www.bsi.bund.de](http://www.bsi.bund.de)
- ISO/IEC 17799  
[www.iso-17799.com/](http://www.iso-17799.com/)
- CoBiT  
[www.isaca.org](http://www.isaca.org)

die selbst den höchsten Anforderungen genügen. Darüber hinaus sind einige unserer Mitarbeiter CISA-zertifizierte Experten (Certified Information System Auditor) und verfügen über die entsprechende Kompetenz und Erfahrung im Umgang solcher Audits und Analysen. Dieses weltweit anerkannte Zertifikat, das von der ISACA (Information Systems Audit and Control Association) ausgestellt wird, prüft die Fähigkeit von IT-Fachleuten in den Bereichen Audit, Controlling und Security von Unternehmensweiten Informatiksystemen.

Zusammenfassend empfiehlt sich für die Erstellung eines IS-Sicherheitskonzeptes die folgende Vorgehensweise:

- Entwicklung einer IS-Sicherheitspolitik
- Auswahl und Etablierung der geeigneten Organisationsstruktur für das Informatiksicherheitsmanagement
- Erstellung des IS-Sicherheitskonzeptes
- Realisierung der Sicherheitsmassnahmen
- Schulung und Sensibilisierung der Anwender
- Aufrechterhaltung der Informationssicherheit im laufenden Betrieb

Auf die Möglichkeiten zur Herleitung von Sicherheitsmassnahmen wird anschliessend in den folgenden Kapiteln detaillierter eingegangen.

## 2 Basis-Services

<b>Modul</b>	<b>Inhalt</b>	<b>Resultate</b>
Basisanalyse	<ul style="list-style-type: none"> <li>• Interner Netzwerk-Scan</li> <li>• Interview mit EDV-Verantwortlichem</li> <li>• Self Assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Audit-Bericht               <ul style="list-style-type: none"> <li>- Beurteilung IST-Zustand</li> <li>- Risikoabschätzung</li> <li>- Massnahmen</li> <li>- Empfehlung weiteres Vorgehen</li> </ul> </li> </ul>
Kundenforum	<ul style="list-style-type: none"> <li>• Vorträge</li> <li>• Präsentationen</li> <li>• Workshop</li> </ul> <p>Inhouse beim Kunden (Kunde stellt Räumlichkeiten und Infrastruktur zur Verfügung)</p>	<ul style="list-style-type: none"> <li>• Event               <ul style="list-style-type: none"> <li>- Übersicht Informatiksicherheit</li> <li>- Rechtliche Aspekte</li> <li>- Präsentation und Diskussion des Audit-Berichts</li> </ul> </li> </ul>

## 2.1 Basisanalyse: Ihre IT-Security im Visier

Neue Informationstechniken wie das Internet und lokale Netzwerke bieten immense Vorteile, aber auch ebenso grosse Risiken. Doch während sich der Nutzen dieser Technologien (Schnelligkeit, problemlose Kommunikation über grosse Entfernungen hinweg, hohe Datenverfügbarkeit etc.) meist schnell manifestiert, sind die Schwachstellen auf den ersten Blick oft nicht zu erkennen. Dabei birgt unzureichende Informatiksicherheit grosse Gefahren in sich, vom unberechtigten Zugriff auf Daten bis hin zur Manipulation von aussen. Je präziser also die Kenntnis des Status Quo Ihrer Informationssysteme, desto effektiver kann sich Ihr Unternehmen schützen.

Ein weiterer Aspekt: Informatiksicherheit ist nicht nur eine Frage des persönlichen Geschmacks, sondern eine rechtliche Notwendigkeit. Gemäss Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 Art. 7 Datensicherheit müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugten Zugriff geschützt werden.

Hier setzt die Basisanalyse an. Sie bietet eine kostengünstige Möglichkeit, den aktuellen Stand der Informatiksicherheit Ihres Unternehmens zu ermitteln. In einem verständlichen Bericht zeigen wir Ihnen die Sicherheitsschwachstellen Ihrer Informationssysteme auf und empfehlen konkrete Massnahmen, um diese zu beheben.

Die Basisanalyse umfasst folgende Teilschritte:

<b>Self Assessment</b>	Dauer:	ca. 0.5 Std.
Anhand einer Checkliste und eines Fragenkatalogs bewerten Sie eigenständig die massgeblichen Sicherheitskomponenten und -massnahmen. Dadurch erhalten Sie auf einfache und effiziente Weise einen guten Überblick über das gesamte Spektrum der Informatiksicherheit.		
<b>Netzwerk-Scan vor Ort</b>	Dauer:	ca. 3 Std.
Ein Sicherheitsspezialist analysiert inhouse Ihre Netzwerkkomponenten (Clients, Server, Betriebssysteme, Kommunikationssysteme, Router etc.). Organisatorische und technische Massnahmen werden auf Anwendbarkeit und Funktionalität überprüft. Zusätzlich überprüft der Experte die Sicherheit Ihrer Web- und E-Mail-Server sowie die zugehörigen Schutzmassnahmen (Firewall, Mail-Security Gateway, etc.).		
<b>Interview mit dem EDV-Verantwortlichen</b>	Dauer:	ca. 1 Std.
Die ersten Resultate und Erkenntnisse werden mit dem EDV-Verantwortlichen diskutiert. Unsere Experten zeigen dabei auf, welche Massnahmen dringend erforderlich sind. Ziel dieses Interviews ist es, zusätzlichen Informationsbedarf der EDV-Abteilung zu decken.		
<b>Audit-Bericht</b>		
Die Auswertung des Self Assessment und des internen Netzwerk-Scans werden in einem aussagekräftigen Bericht zusammengefasst. Dabei werden Ursachen und Folgen der Schwachstellen aufgezeigt. Abschliessend empfiehlt der Experte einen Massnahmenplan, der nach Dringlichkeit priorisiert ist.		

## 2.2 Kundenforum: Informatiksicherheit für Entscheider

Oft gewinnt man den Eindruck, dass Informatiksicherheit nur die EDV-Abteilung betrifft. Doch um umfassende Sicherheit zu garantieren, muss auch die Entscheiderebene und ihre Kontrollorgane miteinbezogen werden. Welche Massnahmen sind nötig? Wieviel Budget steht zur Verfügung? Wie und vom wem werden die Massnahmen kontrolliert? Nur, wenn diese und weitere Prämissen im Vorfeld geklärt sind, kann grösstmögliche Informatiksicherheit garantiert werden - eine Tatsache, der sich viele Entscheider nicht bewusst sind.

Ziel des Kundenforums ist es, dieses Bewusstsein zu schaffen, die Bedeutung der Informatiksicherheit deutlich vor Augen zu führen und das Thema den Entscheidern näher zu bringen.

Im Kundenforum präsentieren wir die erforderlichen Grundlagen und stellen mögliche Auswirkungen von Schwachstellen sowie die rechtliche Situation dar. Anschliessend werden die Erkenntnisse aus der Basisanalyse der internen EDV-Infrastruktur erläutert und die empfohlenen Massnahmen diskutiert.

Die Veranstaltung gliedert sich wie folgt:

<b>Einführung in das Thema „Informatiksicherheit“</b>	Dauer:	ca. 1 Std.
Dem Besucher wird das Thema Informatiksicherheit näher gebracht. Ziel ist es, grundlegende Informationen zu vermitteln.		
<b>Rechtsgrundlagen und Verantwortungen</b>	Dauer:	ca. 0.5 Std.
Der Referent informiert über die aktuellen rechtlichen Anforderungen und zeigt die Auswirkungen von Sicherheitslücken auf.		
<b>Ergebnisse und Empfehlungen auf Grund der Basisanalyse</b>	Dauer:	ca. 0.5 Std.
In diesem Teil werden die Erkenntnisse der Basisanalyse und der aktuelle Status erläutert. Unser Sicherheitsspezialist legt den IST-Zustand Ihrer Informatikstruktur dar und empfiehlt notwendige Massnahmen zur Gewährleistung und Verbesserung der Informatiksicherheit.		
<b>Diskussion der empfohlenen Massnahmen</b>	Dauer:	offen

### 3 Weiterführende Services

Modul	Inhalt	Resultate
Detailanalyse	<ul style="list-style-type: none"> <li>• Benchmark-Analyse (IST-SOLL-Vergleich)</li> <li>• Control Self Assessment (CSA)</li> <li>• Impact-Analysen</li> <li>• Machbarkeitsstudien</li> <li>• Penetration Tests</li> <li>• Risikoanalysen</li> <li>• SAP Security</li> </ul>	<ul style="list-style-type: none"> <li>• Schwachstellen und Ursachen</li> <li>• Massnahmen               <ul style="list-style-type: none"> <li>- kurzfristig</li> <li>- mittelfristig</li> <li>- langfristig</li> </ul> </li> <li>• Umsetzungsplan</li> <li>• Budget, Realisierungskosten</li> </ul>
IS-Sicherheitskonzept (ISK)	<ul style="list-style-type: none"> <li>• Klassifikation von Systemen und Daten</li> <li>• Definition der Schutzziele</li> <li>• Richtlinien für Administratoren und Benutzer</li> <li>• Systemkonfigurationen</li> <li>• Vorgehenspläne</li> </ul>	<ul style="list-style-type: none"> <li>• Anforderungskataloge</li> <li>• Konzepte</li> <li>• Richtlinien</li> <li>• Notfallpläne</li> </ul>

## 3.1 Detailanalysen

### 3.1.1 Benchmark-Analyse: Ihre Sicherheitsziele auf dem Prüfstand

Welche Ziele hat sich Ihr Unternehmen im Bezug auf die Informatiksicherheit gesetzt? Wurde diese Messlatte erreicht? Diese und ähnliche Fragen beantwortet die Benchmark-Analyse. Sie untersucht den Ist-Zustand Ihrer Informatiksicherheit und vergleicht ihn mit den Sollwerten, die Sie definiert haben.

Die Benchmark-Analyse beinhaltet folgende Teilschritte:

---

#### **Definition des Standards**

Haben Sie sich bereits für einen Standard entschieden, so werden hier die relevanten Vergleichskriterien festgelegt. Alternativ: In Abstimmung mit Ihnen wird der Standard festgelegt, der für das Sicherheitsprojekt angewendet werden soll.

---

#### **Interview und Risikoberechnung**

Zur Ermittlung des Ist-Zustandes werden führen wir mit Ihnen ein oder mehrere Interviews. Auf dieser Basis wird das individuelle Sicherheitsrisiko ermittelt.

---

#### **Systemanalyse**

Ein Sicherheitsspezialist katalogisiert vor Ort Ihre Netzwerkkomponenten (Clients, Server, Betriebssysteme, Kommunikationssysteme, Router etc.). Organisatorische und technische Massnahmen werden auf Anwendbarkeit und Funktionalität überprüft.

Zusätzlich wird die Sicherheit Ihrer Web-Server und E-Mail-Server und deren Schutzeinrichtungen (Firewall, Mail-Security Gateway, etc.) überprüft.

---

#### **Dokumentation**

Die Ergebnisse des Vergleichs werden dokumentiert, auf dieser Basis werden geeignete Massnahmen empfohlen.

---

### **3.1.2 Control Self Assessment (CSA): Sehen Sie die Sicherheit Ihres Unternehmens mit anderen Augen**

Keiner kennt sein Unternehmen so gut wie Sie selbst, doch ein Aussenstehender entdeckt oft neue Aspekte. Auf dieser Erkenntnis basiert das Modul CSA, die „gelenkte Selbsteinschätzung“. Die Verantwortlichen selbst beurteilen die Kontrollmechanismen Ihres Unternehmens, dabei werden Sie durch unsere Sicherheitsexperten durch gezielte Moderation unterstützt. Dadurch wird sichergestellt, dass die gesamte Bandbreite der Informatiksicherheit berücksichtigt wird.

Inhalte einer geführten Selbsteinschätzung:

---

#### **Moderation**

Der Moderator stellt verschiedene Sicherheitsaspekte vor, die er jeweils mit Ihnen diskutiert. Auf dieser Basis werden Schwachstellen ermittelt und protokolliert.

---

#### **Dokumentation**

Auf Grundlage des Protokolls dieser gesteuerten Diskussion wird der IST-Zustand schriftlich festgelegt.

Wir geben Ihnen Empfehlungen zum weiteren Vorgehen und erforderlichen Sicherheitsmassnahmen ab.

---

### 3.1.3 Impact Analysis: Der Sicherheitsspielraum Ihrer IT

Die Impact Analysis zeigt auf, über welchen „Sicherheitspuffer“ Ihr Unternehmen verfügt. Anders gesagt: Wie stark wird die Geschäftskontinuität beeinträchtigt, wenn Sicherheitsmassnahmen abgebaut werden?

Auf Basis dieser Analyse lässt sich das Risikopotenzial des Unternehmens abschätzen. Unter Berücksichtigung des Kosten-/Nutzenverhältnisses und unter sorgfältiger Abwägung der Sicherheitsaspekte wird so das Restrisiko beurteilt.

Diese Einflussanalyse gliedert sich folgendermassen:

---

#### **Sukzessives Ausschalten der Sicherheitsmassnahmen**

In einem Planspiel werden die vorhandenen Sicherheitsmassnahmen Schritt für Schritt ausgeschaltet.

Bei jedem Schritt wird untersucht, wie das Gesamtsystem reagiert.

---

#### **Dokumentation**

In der Dokumentation werden diese einzelnen Schritte sowie die zugehörigen Systemeigenschaften beschrieben.

Die Grenze der Systemstabilität und -verfügbarkeit wird dadurch klar definiert und dokumentiert.

---

### 3.1.4 Machbarkeitsstudie: Frühzeitige Analysen zur Risikominimierung

Die Konzeption und/oder Implementierung einer neuen Sicherheitslösung sowie das Changemanagement bringen immer ein sehr hohes Risiko mit sich. Es kann zu Beeinträchtigungen der Abläufe kommen, im schlimmsten Fall (worst case) läuft das gesamte System nach der Änderung nicht mehr oder die Integration eines neuen Systems in ein bestehendes Informatikumfeld ist unmöglich.

Um solche Beeinträchtigungen/Ausfälle zu vermeiden, identifiziert die Machbarkeitsstudie kritische Bereiche bereits im Vorfeld.

Die Machbarkeitsstudie beinhaltet folgende Teilschritte:

---

#### **Bestandsaufnahme der bestehenden Umgebung**

Das gesamte Informatikumfeld, das von der Systemintegration oder der Neurealisierung betroffen ist, wird erfasst und dokumentiert.

---

#### **Definition der Lösung**

In einem Gespräch und/oder einer Analyse ermittelt der Sicherheitsfachmann die Anforderungen, die an die neue Lösung gestellt werden.

Die Gründe für den Einsatz neuer Technologien, Hard-/Software Komponenten werden in die Überlegungen miteinbezogen.

---

#### **Analyse der Integration in das bestehende Informatikumfeld**

Der Experte erstellt eine Analyse, die zeigt, wie die neuen Komponenten integriert werden können, und definiert – auf Basis der technischen Anforderungen - den Machbarkeitsgrad.

In dieser Phase wird beschrieben, welche Anforderungen das System erfüllen muss, um den gewünschten Machbarkeitsgrad zu erreichen.

Liegt der Machbarkeitsgrad unterhalb eines vorher definierten Mindestwertes, wird die Implementierung als nicht realisierbar eingestuft. Die Begründung für diese Einstufung werden ebenfalls dokumentiert.

---

### 3.1.5 Penetration Test: Mehr Sicherheit durch „simulierte“ Attacken

Mit dem verstärkten Einsatz von Informations- und Kommunikationsmedien steigt die Gefahr des unerlaubten Eindringens in diese Systeme. Angreifer nutzen entweder technische Mängel und/oder das menschliche Verhalten aus.

Um von technischer Seite möglichst wenig Angriffsfläche zu bieten, werden z. B. Antivirus-Software, Firewalls und weitere Hilfsmittel eingesetzt. Doch trotz dieser Schutzmassnahmen gelingt es immer wieder, in die Systeme einzudringen – etwa, wenn die Schutzmassnahmen nur Teilbereiche abdecken oder die individuellen Sicherheitsanforderungen des Unternehmens unzureichend erfüllen.

Der zweite Ansatzpunkt: Im Alltagsgeschäft neigen Menschen oft zu einer gewissen Nachlässigkeit, etwa, wenn die Notwendigkeit der Massnahmen nicht deutlich vermittelt wurde. Dieses fehlende Gefahrenbewusstsein wie auch mangelnde Sicherheitsvorkehrungen im organisatorischen Bereich führen dazu, dass technische Sicherheitsmassnahmen einfach umgangen werden.

Penetration Tests decken solche Schwachstellen auf.

---

#### **Definition des zu penetrierenden Bereichs**

Gemeinsam mit Ihnen werden die Art des Penetration Tests und die zu überprüfenden Bereiche definiert.

Diese Vereinbarung wird vertraglich festgehalten.

---

#### **Durchführung des Penetration Tests**

Mit Hilfe von Tools und Strategien werden die Informationssysteme attackiert. Die Resultate der Attacken werden dokumentiert.

Generell lässt sich unterscheiden zwischen:

##### **White Box-Test:**

Sie stellen eine Beschreibung des Ist-Zustands und eine Dokumentation der Informatikumgebung zur Verfügung. Falls die Dokumentation fehlt, wird diese in Zusammenarbeit mit Ihnen erstellt. Anschliessend werden die vorher definierten Penetration Tests durchgeführt.

##### **Black Box-Test:**

Alle notwendigen Informationen über die vorhandene Informatik-Infrastruktur werden ohne Mithilfe Ihrerseits zusammengetragen. Dieses Vorgehen ist zwar meist aufwändiger, entspricht jedoch exakt dem eines möglichen Angreifers. Nach der Informationsbeschaffung werden die vereinbarten Attacken ausgeführt.

---

#### **Dokumentation**

Die Resultate und die empfohlenen Massnahmen werden in einem Bericht dokumentiert.

---

### 3.1.6 Risikoanalyse: Der gezielte Gefahrencheck

Die Risikoanalyse untersucht einzelne Bereiche der Informationssysteme, die drei Hauptbereiche sind Recht, Organisation und Technik. Dabei kann die Analyse nach internationalen, nationalen, kantonalen oder unternehmenseigenen Standards durchgeführt werden. Als Ergebnis legen wir eine Dokumentation vor, die das Risikopotenzial des jeweiligen Gebietes darstellt.

Diese Risikoanalyse beinhaltet folgende Teilschritte:

---

#### **Definition des Standards**

Sie und der Spezialist entscheiden gemeinsam, welcher Standard bei der Risikoanalyse angewendet wird.

---

#### **Interview und Risikoberechnung**

Zur Ermittlung des Risikopotenzials führt der Sicherheitsexperte mit Ihnen ein oder mehrere Interviews.

Auf dieser Basis wird die Bedeutung des jeweiligen Bereichs sowie der Status Quo der vorhandenen Sicherheitsinfrastruktur bestimmt.

Anhand dieser beiden Werte wird das Risiko ermittelt.

---

#### **Dokumentation**

Je nach Vereinbarung erhalten Sie eine komprimierte Dokumentation mit den Risikoresultaten inkl. grafischer Darstellung oder eine umfassende Dokumentation mit Ursachenbeschreibung und Empfehlungen.

---

### **3.1.7 SAP-Security: Komplexe Anforderungen, präzise Lösungen**

SAP ist die Software-Lösung, die im Bereich ERP und Finanzwesen am weitesten verbreitet ist.

Die Erfüllung der Sicherheitsanforderungen ist hier von besonders grosser Bedeutung, da die Berechtigungskonzepte äusserst komplex sind und auf eine Datenbank mit einem höchst sensiblen Datenbereich zugegriffen wird.

Die SAP-Security Services berücksichtigen diese Prämissen.

---

#### **Zugriffsberechtigungen**

Ein Sicherheitsfachmann analysiert das Berechtigungskonzept und seine Implementierung.

---

#### **Datensicherheit**

Die Daten und ihr Schutz vor unerlaubten Zugriffen werden analysiert.

Der Spezialist überprüft die Einhaltung der Anforderungen an die Datenintegrität und –  
vertraulichkeit.

---

#### **Verfügbarkeit**

Die Systemverfügbarkeit sowie die SLAs (Service Level Agreements) werden untersucht.

---

#### **Dokumentation**

Die Resultate werden in einer Dokumentation zusammengefasst.

---

## 3.2 IS-Sicherheitskonzept: Sicherheit in allen Unternehmensbereichen

### 3.2.1 Ausgangspunkt: „Informatiksicherheit“ – eine ganzheitliche Aufgabe

Die Gewährleistung der Informatiksicherheit ist eine sehr aufwändige Aufgabe. Sie betrifft nicht nur die technische Seite, sondern praktisch alle Bereiche, z. B. die Organisationsstrukturen, das Verhalten der Mitarbeiter, das Know-how etc. – und das aus gutem Grund: Heute sind Unternehmen immer mehr von der Informatik abhängig.

Daher spielen Informationssysteme und ihr Schutz eine immer grössere Rolle und tragen entscheidend zum Unternehmenserfolg und der Wettbewerbsfähigkeit bei. Meist ist zwar der direkte Nutzen von Sicherheitsmassnahmen nicht sofort ersichtlich, doch Lücken im System können grossen Schaden anrichten. Zudem bestehen heute gesetzliche Regelungen (DGB, OR usw.), die den Entscheidern Verantwortung für die Informatiksicherheit zuweisen. Umso wichtiger ist ein gesamtheitliches IS-Sicherheitskonzept.

### 3.2.2 Die richtige Basis: Ein ausgefeiltes Sicherheitskonzept

Dieses IS-Sicherheitskonzept besteht aus mehreren Modulen (Bausteinen), die alle kritischen Unternehmensbereiche abdecken und nach dem „Top-down“-Ansatz implementiert werden.

Wichtig: Die Erstellung eines solchen Konzeptes darf keine einmalige Tätigkeit sein, sondern ist vielmehr ein fortwährender Prozess. Denn wächst ihr Unternehmen, muss die Informatiksicherheit mitwachsen – und veraltete Systeme stellen ein Sicherheitsrisiko dar.

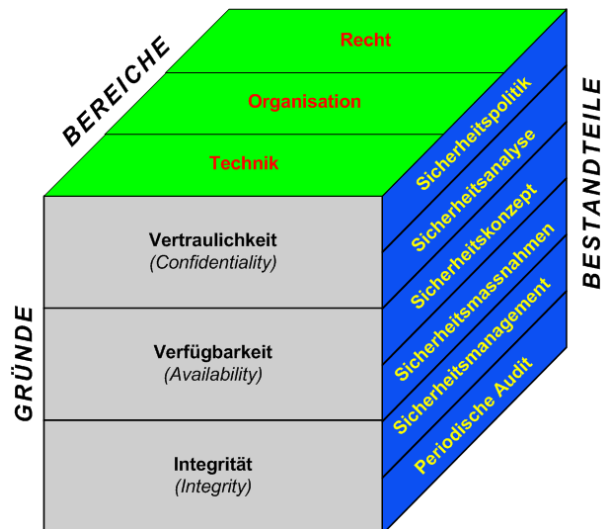


Abbildung 4: Bestandteile des IS-Sicherheitskonzepts

### 3.2.3 Schritt für Schritt zum umfassenden Sicherheitskonzept

Wir empfehlen die folgende Vorgehensweise für die Erstellung eines solchen Informatiksicherheitskonzepts:

- Entwicklung einer Sicherheitspolitik
- Auswahl und Etablierung der Organisationsstruktur
- Erstellung der einzelnen Sicherheitskonzepte und Richtlinien
- Realisierung der Sicherheitsmassnahmen
- Schulung und Sensibilisierung der Anwender
- Aufrechterhaltung der Sicherheit im laufenden Betrieb
- Periodische Überprüfungen

Die Grafik zeigt die wesentlichen Massnahmen, die erforderlich sind, um die Sicherheit von IS-Systemen zu gewährleisten – eine ausgewogene Mischung aus organisatorischen und technischen Schutzmassnahmen.

In erster Linie werden diese Massnahmen aus bereits beschriebenen „Baselines“ abgeleitet, die von verschiedenen Institutionen aufgestellt wurden und zum grossen Teil kostenlos erhältlich sind. Diese „Baselines“ definieren Methoden zur Analyse, Aufbau und Implementierung von Sicherheitsrichtlinien.

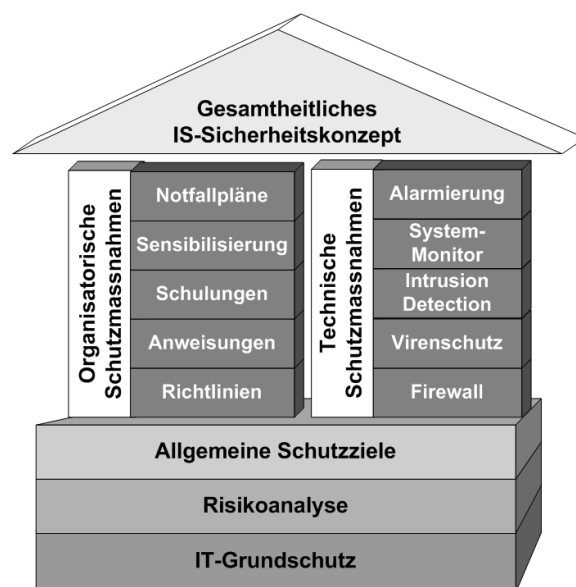


Abbildung 5: Gesamtheitliches IS-Sicherheitskonzept

#### Baselines

- Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik (BSI)
- ISO/IEC 17799 (ehemals Best Code of Practice BS7799-1/ und BS7799-2 der British Standard Organisation)
- CoBit

Dieser „Grundschutz“ wird anhand einer Gefährdungsanalyse, den allgemeinen Schutzziele und den spezifischen Bedürfnissen der Organisation erweitert. Darauf basierend werden individuelle Richtlinien erstellt und davon organisatorische und technische Massnahmen abgeleitet.

## 4 Periodische Services

<b>Modul</b>	<b>Inhalt</b>	<b>Resultate</b>
Periodisches Audit	Überprüfung von: <ul style="list-style-type: none"><li>• Verträgen (SLAs)</li><li>• Richtlinien<ul style="list-style-type: none"><li>- intern</li><li>- extern</li></ul></li><li>• Prozessmanagement</li><li>• Personelle Sicherheit</li><li>• Technische Infrastruktur</li></ul>	<ul style="list-style-type: none"><li>• Auditbericht</li><li>• Bewertung</li><li>• Massnahmen</li></ul>

## 4.1 Periodisches Audit: Kontinuierliche Sicherheit im dynamischen IT-Umfeld

Die Realisierung von Security-Massnahmen alleine genügt nicht. Im sich rasch ändernden Umfeld der EDV-Technologien ist es unumgänglich, die eingesetzten Kontrollmechanismen regelmässig zu überwachen und zu überprüfen. Wir bieten periodische Audits, die eine grösstmögliche Aktualität der Sicherheitsmassnahmen garantieren.

Die Resultate dieses Audits werden in einem verständlichen Bericht abgefasst und zusammen mit den empfohlenen Optimierungsmassnahmen dargestellt.

Das periodische Audit beinhaltet eine Überprüfung der folgenden Bereiche:

---

### **Juristisch (Rechtliche Aspekte)**

Überprüfung von Verträgen mit Drittfirmen und Outsourcing-Partnern

Überprüfung von Dienstleistungsbeschreibungen und Service Level Agreements

Überprüfung des IS-Sicherheitskonzepts (Informatiksicherheitskonzepts?)

---

### **Organisatorisch**

Analyse der implementierten Prozesse und die Beurteilung ihrer Effizienz und Effektivität

Beurteilung des Prozessmanagements

Überprüfung aller Dokumentationen

---

### **Technisch**

Die Überprüfung der technischen Konsistenz des Systems

Audition der Zuverlässigkeit und Verfügbarkeit

Kontrolle der gesamten technischen Infrastruktur zur Gewährleistung der Geschäftskontinuität

---

## 5 Begleitende Services

Modul	Inhalt	Resultate
Coaching / Controlling	<ul style="list-style-type: none"> <li>• Persönliche Betreuung</li> <li>• Periodische Sitzungen</li> <li>• Dokumentation</li> </ul>	<ul style="list-style-type: none"> <li>• Begleitung der Umsetzung</li> <li>• Überprüfung               <ul style="list-style-type: none"> <li>- Realisierungsmassnahmen</li> <li>- Budget</li> <li>- Planung</li> </ul> </li> <li>• Vermitteln von Fachwissen</li> </ul>
Schulung / Workshop	<ul style="list-style-type: none"> <li>• Sensibilisierung von               <ul style="list-style-type: none"> <li>– Management</li> <li>– Mitarbeitern</li> </ul> </li> <li>• Einführung in die Informatiksicherheit</li> <li>• Themenwunsch des Kunden</li> <li>• Nachdiplom-Studium (NDS) Information Security Management</li> </ul>	<ul style="list-style-type: none"> <li>• Massnahmenplan</li> <li>• Schulungskonzept</li> <li>• Bedürfniskonforme Aus- und Weiterbildung</li> <li>• Durchgeführte Schulung / Workshop</li> <li>• Schulungsunterlagen</li> </ul>
Pflichtenheft / Evaluation	<ul style="list-style-type: none"> <li>• Bedarfsanalysen</li> <li>• Definition der Anforderungen</li> <li>• Durchführen der Evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Pflichtenheft</li> <li>• Ausschreibung / Offertanfragen</li> <li>• Evaluation</li> </ul>

## 5.1 Schulungen/Workshops: Fundiertes Know-how für alle Bereiche

Wir haben ein umfassendes Angebot von Schulungen, Workshops oder Seminaren entwickelt, die intern (beim Kunden) oder extern stattfinden. Neben den unten aufgeführten Themen bieten wir Veranstaltungen an, die individuell für Ihre Fragestellungen konzipiert werden.

Unser Portfolio umfasst Veranstaltungen für unterschiedliche Zielgruppen zu folgenden Themen:

---

### Management / Kader

- Gruppendynamische Prozesse
- Security Management
- Führung
- Prozess-Management
- Projekt-Management
- Security Awareness
- Public Key Infrastructure

---

### Anwender

- Security Awareness
- Anwenderunsicherheit
- Was kann ich mit meinen Handlungen bewirken?

---

### IT-Administratoren

- Internet/Intranet Security
- Firewall Security
- Messaging Security
- SAP Security
- Kryptographie
- Public Key Infrastructure

---

### Individuelle Workshops/Seminare

Themen werden speziell auf Ihre Bedürfnisse abgestimmt.

---

## 5.2 Pflichtenheft / Evaluation: Das Komplettangebot rund um das Einholen von Angeboten

Je präziser die Sicherheitsziele eines Unternehmens definiert sind, desto gezielter lassen sich seine individuellen Anforderungen erfüllen – unnötiger Arbeits- und Kostenaufwand kann vermieden werden. Ein Pflichtenheft ist eine wichtige Grundlage, um diese herauszufinden und eine Ausschreibung oder Offertanfrage bei Lieferanten und/oder Herstellern durchzuführen. Als Grundlage werden zunächst die entsprechenden Anforderungen verifiziert bzw. definiert und die Ziele in MUSS- und KANN-Ziele eingeteilt. Auf dieser Basis wird das Pflichtenheft erstellt.

Die Evaluation beginnt mit einer groben Selektion der Offerten. Die angebotenen Produkte und Dienstleistungen werden anhand von erstellten Kriterienkatalogen bewertet und beurteilt. Auf dieser Basis und anhand einer Nutzwertanalyse wird ein Realisierungspartner vorgeschlagen.

Das Angebot umfasst folgende Leistungen:

---

### **Pflichtenheft**

- Verifizieren der Anforderungen
- Aufnahme der detaillierten Bedürfnisse
- Definition von MUSS-, resp. KANN-Zielen
- Erstellen des Pflichtenhefts

---

### **Ausschreibung**

- Ausarbeiten von Vorlagen und Dokumenten zur effizienten Evaluation des Realisierungspartners
- Vornehmen der Ausschreibung
- Versenden des Pflichtenhefts an die Interessenten
- Beantworten von Fragen der Interessenten in einer Stellungnahme

---

### **Evaluation**

- Sichten und Beurteilen der eingegangenen Angebote
  - Erstellen des Fragenkatalogs zu den eingegangenen Angeboten
  - Versenden von Information und Fragenkatalog, resp. Absage an die Anbieter
  - Bewerten der Vollständigkeit
  - Überarbeiten der zweiten Angebote, die auf Grund der Fragen angepasst wurden
  - Organisation von und Teilnahme an Anbieterpräsentationen
  - Beurteilen der Angebote und Empfehlung zur Wahl des Realisierungspartners
-