

# Rollen für Informationssicherheit in einer Best-Practice-Organisation

Wolfram Funk <sup>1</sup>

**Einordnung:** Unternehmen benötigen eine Sicherheitsorganisation und Prozesse, um Maßnahmen zur Informations- oder IT-Sicherheit definieren, implementieren und kontrollieren zu können. Damit ein derartiges Informationssicherheitsmanagementsystem (ISMS) effektiv arbeiten und den Anforderungen an die Sicherheit Rechnung tragen kann, muss die Verantwortung dafür in der Führungsstruktur des Unternehmens verankert sein. Hierfür bieten sich, abhängig von der Größe und Struktur des Unternehmens, unterschiedliche Rollenmodelle an.

**Schlüsselwörter:** Informationssicherheit; Informationssicherheitsmanagement; Sicherheitsorganisation; Rollen; Chief Information Security Officer; Chief Security Officer

---

## Abstract

Die Reife eines Unternehmens im Hinblick auf den Umgang mit Informationssicherheit hängt sehr stark von der Art ab, wie diese organisatorisch im Unternehmen verankert ist. Dabei geht es vor allem um Prozesse des Informationssicherheitsmanagements und um die Verantwortlichkeiten im Umfeld der Informationssicherheit. Die ISO 27001:2005 beziehungsweise ISO 27002:2005 als detaillierte Referenznorm gibt den groben Rahmen unter anderem für die Organisation von Informationssicherheit im Unternehmen und mit Blick auf externe Partner vor. Sie lässt jedoch offen, wie im Einzelnen die Rollen verteilt sein sollen. Die Zuweisung und Wahrnehmung von Verantwortlichkeiten ist aber entscheidend, da geschäftliche Entscheidungen zu treffen sind hinsichtlich der aufzuwendenden Mittel einerseits und des als adäquat angestrebten Sicherheitsniveaus andererseits. Da jedes Unternehmen andere Ausgangsvoraussetzungen mitbringt, gibt es hierfür kein Patentrezept, wohl aber Best-Practices. Der Beitrag zeigt, wie Informationssicherheit von den unterschiedlichen Führungspositionen wahrgenommen und bewertet wird und stellt dem Empfehlungen für Rollenmodelle gegenüber. Auf Spezifika beim Mittelstand wird hingewiesen. Den Empfehlungen werden abschließend die Ergebnisse einer Erhebung in deutschen Unternehmen gegenübergestellt. Die Diskrepanzen sind teilweise deutlich.

---

1 Kontakt per E-Mail: [wolfram.funk@experton-group.com](mailto:wolfram.funk@experton-group.com) und [funk@wolframict.com](mailto:funk@wolframict.com)



**Wolfram Funk** bietet geschäftsorientierte Beratung für Unternehmen, die ICT-Lösungen<sup>2</sup> erfolgreich entwickeln und vermarkten oder in ICT-Anbieter investieren möchten; er unterstützt beim Risiko- und Informationssicherheitsmanagement und ist als unabhängiger Analyst für Informationssicherheit für Meinungsbildner und Institutionen tätig; Wolfram Funk ICT Business Consulting ist Kooperationspartner der Experton Group; Herr Funk war als Senior Advisor bei Experton Group, als Senior Consultant und Analyst bei META Group Deutschland sowie bei der Xcc Software AG in Vertrieb und Marketing tätig.

## Einleitung

Um die Wirksamkeit und Effizienz des Informationssicherheits-Managements im Unternehmen zu verstehen, müssen die unterschiedlichen Perspektiven auf Informationssicherheit verstanden werden. Dabei muss zum einen geklärt werden, wie die Rollen für Informationssicherheit verteilt sind und wie weit die Entscheidungskompetenzen jeweils gehen. Zum anderen muss ein gemeinsames Verständnis für Informationssicherheit im Unternehmen entwickelt werden. Ein weiterer kritischer Punkt ist die Kommunikation zwischen den einzelnen Funktionen, Bereichen bzw. Rollen. Dass diese Fragen nicht trivial zu lösen sind, wird bei einer genaueren Betrachtung der unterschiedlichen Perspektiven auf Informationssicherheit innerhalb eines Unternehmens deutlich.

## Inhaltsverzeichnis

<b>1. Unterschiedliche Perspektiven auf Informationssicherheit .....</b>	<b>3</b>
<b>2. Aufgabenverteilung in einer Best-Practice-Sicherheitsorganisation .....</b>	<b>4</b>
<b>3. Die Realität .....</b>	<b>6</b>
<b>4. Spezifische Rahmenbedingungen im Mittelstand.....</b>	<b>6</b>
<b>5. Zusammenfassung.....</b>	<b>7</b>
<b>6. Literatur .....</b>	<b>7</b>

---

2 ICT: Information and Communication Technology (engl.) bzw. Informations- und Telekommunikationstechnologie

## 1. Unterschiedliche Perspektiven auf Informationssicherheit

Informationssicherheit ist Chefsache. Allerdings wird die Relevanz des Themas von den einzelnen Funktionen bzw. Akteuren innerhalb der Unternehmensführung und betrieblichen Funktionsbereichen typischerweise recht unterschiedlich bewertet.

So räumen Vorstand oder die Geschäftsführung (**CEO**) der wirtschaftlichen Entwicklung des Unternehmens höchste Priorität ein. Wenn Maßnahmen der Informationssicherheit dies unterstützen, sind sie willkommen – vorausgesetzt, dass der Nutzen in einer positiven oder zumindest neutralen Relation zu den Kosten steht. Wichtige Nutzenaspekte sind dabei: 1) Reduzierung oder Vermeidung von Risiken, 2) interne Prozessoptimierung, 3) Förderung der Geschäftstätigkeit und 4) positive Beeinflussung der Reputation des Unternehmens und Übernahme gesellschaftlicher Verantwortung.

Die Verantwortlichen für das unternehmensweite Risikomanagement (Chief Risk Officer, **CRO**) möchten Bedrohungen, Schwachstellen und Risiken für das Unternehmen verstehen, Risiken bzw. das Restrisiko so weit wie möglich kalkulierbar machen, die Höhe der Risikoakzeptanz festlegen, Prioritäten bei Sicherheitsmaßnahmen setzen, Investitionen in Sicherheitsmaßnahmen rechtfertigen und letztlich das Sicherheitsbewusstsein im Unternehmen erhöhen.

In der Position des **CCO** (Chief Compliance Officer bzw. die Rechtsabteilung) wird allgemein die Einhaltung von Regularien gefordert. Der Einsatz von Informationstechnologie muss mit rechtlichen Anforderungen konform sein. Er kann darüber hinaus die Verwaltung regulatorischer Vorgaben automatisieren. Die Schnittstelle zur IT liegt in der Regel in den Bereichen Informationsschutz, Risikomanagement, Informationsmanagement, internes Kontrollsystem sowie in Mitwirkungs- und Informationspflichten.

Die Finanzleitung (Chief Financial Officer, **CFO**) erwartet von Maßnahmen der Informationssicherheit, dass sie möglichst kosteneffizient gestaltet werden und mit Blick auf die Abwehr von Risiken einen hohen Nutzenbeitrag bringen. Außerdem sollen die Maßnahmen an sich kosteneffizient umgesetzt werden.

Der **CISO** (Chief Information Security Officer) sorgt für die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, und er ist zuständig für das (IT-) Risikomanagement. Hierüber besteht in der Regel ein Konsens. Die tatsächliche Ausprägung und Entscheidungskompetenz der CISOs in deutschen Unternehmen ist jedoch sehr unterschiedlich. Sie variiert zwischen zwei Extremen: dem CISO, der eher auf Business-Seite angesiedelt ist und relativ weit weg von IT-Themen ist, und dem CISO innerhalb der IT-Organisation, der eigentlich IT-Security-Manager ist und sich ausschließlich mit informationstechnischen Fragestellungen und allenfalls nebenbei mit IT-Risikomanagement befasst. Die zweite Konstellation ist in der Praxis häufiger zu finden.

Die IT-Leitung (Chief Information Officer, **CIO**) leistet ihren Beitrag zur Unterstützung des operativen Geschäfts. IT-Sicherheit ist dabei nur eines von vielen Themen und steht im Hinblick auf die Budgetzuteilung im Wettbewerb mit anderen Vorhaben. Sicherheitsmaßnahmen sollen aus Sicht des CIO daher kosteneffizient sein, das IT-Business-Alignment unterstützen und den IT-Betrieb nicht über Gebühr stören.

Besonders in kleinen und mittelständischen Unternehmen liegen IT- und IT-Sicherheitsfragen häufig in der Verantwortung von Systemadministratoren. Diese sind in der Regel notorisch überlastet und haben wenig Spielraum, um Informationssicherheit strategisch zu adressieren. Dort überwiegt der Grundsatz: „Never change a running system“. Es werden also typischerweise primär jene Sicherheitsaufgaben adressiert, die branchenübergreifend als Minimalstandard gelten – oder leicht zu lösende Sicherheitsprobleme betreffen.

Die einzelnen Geschäftsbereiche eines Unternehmens (Lines of Business, **LOB**) haben ihre spezifischen Zielvorgaben wie Umsatzwachstum und –höhe zu erfüllen. Ähnlich wie auf Vorstandsebene stellt sich hier die Frage nach dem Nutzenbeitrag von Informationssicherheit – allerdings in einer mehr operativen Ausprägung. Ein wichtiges Stichwort ist dabei der Schutzbedarf der einzelnen „Assets“ (Werte wie Informationen, Prozesse, Güter), die im Verantwortungsbereich des LOB-Managements liegen.

Wegen des Einflusses auf die Umsetzung sei zuletzt an die Vielzahl der Endnutzer erinnert. Sie haben oftmals geringe Berührungspunkte zur Informationssicherheit. Sicherheitsmaßnahmen werden dort bisweilen als Zwang oder produktivitätshemmend empfunden. Firmeninterne Kampagnen zur Steigerung des Sicherheitsbewusstseins dienen der Aufklärung und der Schaffung einer positiven Haltung gegenüber Sicherheit und der dafür erforderlichen Maßnahmen.

## 2. Aufgabenverteilung in einer Best-Practice-Sicherheitsorganisation

Die Realisierung von Informationssicherheit umfasst Maßnahmen und Konzepte, die im Spannungsfeld zwischen Business und IT sowie zwischen operativen und strategischen Abläufen angesiedelt sind. Für eine optimale Umsetzung von Informationssicherheit müssen Aufgaben und Verantwortlichkeiten definiert und organisatorisch verankert werden. Nachfolgend werden ausgewählte Rollen bezüglich der Informationssicherheit im Sinne einer Empfehlung näher charakterisiert. Unternehmen sollten ihre Organisation und die Zuweisung von Aufgaben und Verantwortlichkeiten daran ausrichten.

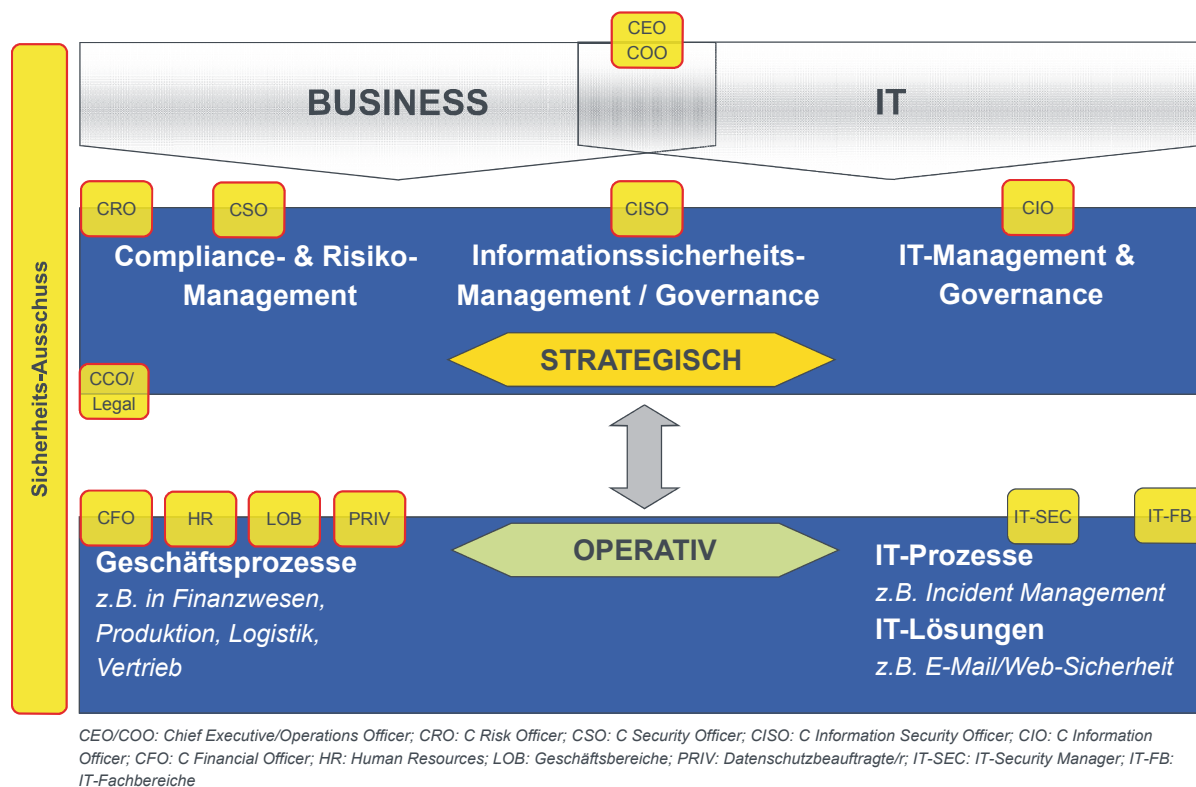


Abb. 1: Rollen für Informationssicherheit in einer Best-Practice-Organisation

### Chief Information Security Officer (CISO)

Der CISO ist grundsätzlich zuständig für das Aufsetzen eines ISMS mit dem Zusatzauftrag Security-Governance. Er ist die zentrale Instanz, der alle Fäden mit Blick auf Informationssicherheit zusam-

menhält. Seine Rolle ist vor allem strategischer und koordinierender Natur, und er bewegt sich an der Schnittstelle zwischen IT und Business (siehe Abb. 1).

Typische Aufgaben sind:

- Security-Strategie entwickeln, Security-Programme und -Initiativen steuern, Koordination mit Geschäftsprozesseignern, Informationsklassifizierung anstoßen,
- Risiko- und „Business Impact“-Bewertungen durchführen, Strategien zur Eindämmung von Risiken entwickeln und mit dem Corporate Risk Management koordinieren, Richtlinien und Compliance durchsetzen,
- Nutzung und Effektivität von Security-Ressourcen überwachen, externe Auditoren einbeziehen,
- Entwickeln und Implementieren von Monitoring- und Metrik-Ansätzen,
- Methoden für die Erfassung und –verteilung von Security-Know-how entwickeln, Security-Metriken zur Effektivitäts- und Effizienzmessung aufstellen,
- Abstimmung mit allen Beteiligten, Lücken und Überlappungen adressieren.

Der CISO sollte außerhalb des IT-Bereichs und auf gleicher Ebene wie der CIO angesiedelt sein. Er berichtet im Idealfall direkt an den Vorstand (CEO) oder an den Verantwortlichen für das unternehmensweite Risikomanagement (CRO). Wichtig ist ein starker Rückhalt durch die Vorstandsebene, denn einige Sicherheitsmaßnahmen müssen im IT-Bereich um- und durchgesetzt werden. Ohne die erklärte, aktive Unterstützung seitens des Top-Managements läuft der CISO Gefahr, im IT-Bereich „aufzulaufen“. Für strategische Maßnahmen muss dem CISO ein eigenes Budget zugeordnet werden.

### **Chief Executive Officer (CEO, Vorstand, Geschäftsführung) und mittleres Management**

Der CEO muss sich ausdrücklich und für alle Mitarbeiter sichtbar zur Wichtigkeit der Informationssicherheit bekennen. Die symbolische Wirkung ist nicht zu unterschätzen. Außerdem muss er direkt oder über das mittlere Management sicherstellen, dass die Arbeit des CISOs nicht behindert wird. Gleichzeitig hat der CEO die Aufgabe, gewisse Obliegenheiten vom CISO einzufordern. Dies sind zum Beispiel die Ausrichtung aller Maßnahmen auf strategische Ziele, die Berücksichtigung von Richtlinien sowie von Vorgaben regulatorischer Art (Compliance) oder für das Risikomanagement. Auch Berichte zu Risikoanalysen sowie zu den Kosten und der Wirksamkeit und Effizienz von Sicherheitsmaßnahmen sind einzufordern. Operativ umgesetzt werden diese Kontrollmaßnahmen gegebenenfalls durch spezifische Rollen wie den Finanzleiter (CFO) oder die Verantwortlichen für Rechtsfragen (CCO) und Risikomanagement (CRO).

### **CIO und IT-Fachbereiche**

Der IT-Leiter oder CIO sowie einzelne Funktionen innerhalb des IT-Bereichs sind relevant für die technische Umsetzung der Sicherheitsmaßnahmen. Größere Unternehmen werden einen IT-Security-Manager mit einem kleinen Team etablieren. Es kümmert sich beispielsweise darum, dass die zur Minderung bestimmter Risiken notwendigen Technologien und die passenden Anbieter identifiziert und bewertet werden. Das Team sorgt auch dafür, dass Sicherheitslösungen in die bestehende IT-Infrastruktur integriert werden. Außerdem stellt der CIO höchstmögliche Kosteneffizienz sicher, auch unter Berücksichtigung von Outsourcing-Optionen.

### **Geschäftsbereichsleiter (Lines of Business – LOBs)**

Die einzelnen Geschäftsbereiche sind die direkten Nutznießer eines guten ISMS. Schließlich geht es bei Informationssicherheit um den Schutz von Informationen und geistigem Eigentum sowie von Geschäfts- oder Produktionsprozessen. Die Rolle der Geschäftsbereiche besteht vor allem darin, die „Informationsgüter“ im eigenen Verantwortungsbereich zu identifizieren und dafür die „Eigentümerschaft“ zu übernehmen. Die Geschäftsbereichsleiter unterstützen bei der Klassifizierung ihrer „Information Assets“

und definieren jeweils die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit für jede Informationskategorie bzw. bestimmte Geschäftsprozesse.

### **Der Sicherheitsausschuss (Security Steering Committee)**

Die Etablierung eines Sicherheitsausschusses ist ein wesentlicher Erfolgsfaktor für den CISO. Dabei handelt es sich um ein Forum für leitende Fachkräfte aus verschiedenen Bereichen des Unternehmens, die alle durch die Art des Umgangs mit Informationssicherheit betroffen sind. Auch ein Mitglied des Vorstands sollte dort vertreten sein. Der CISO kann über das Security-Steering-Committee kontinuierlich die Anforderungen an Sicherheit auf Geschäftsseite aufnehmen, sein Programm daran ausrichten, das Bewusstsein für Informationssicherheit weiter vorantreiben und Unterstützung für seine Vorhaben gewinnen. Der Ausschuss sollte sich regelmäßig treffen, am besten mehrmals jährlich und zusätzlich bei Eintreten wichtiger geschäftlicher Änderungen.

Typische Aufgaben des Sicherheitsausschusses sind:

- Review der Security-Strategie, Integration, Unterstützung der „Business Owner“ einholen,
- neue Risiken und Compliance-Probleme identifizieren, Security-Praktiken in Geschäftsbereichen vorantreiben,
- Eignung von Sicherheitsinitiativen für Geschäftsfunktionen prüfen,
- Review von Security-Aktivitäten vor dem Hintergrund von Geschäftszielen,
- Überprüfung von Prozessen für die Wissenserfassung und –verteilung,
- kritische Geschäftsprozesse und Rollen identifizieren, Integrationsbemühungen vorantreiben bzw. delegieren.

## **3. Die Realität**

Die Relevanz des Themas Informationssicherheit wird von den einzelnen Funktionen und Akteuren innerhalb eines Unternehmens recht unterschiedlich bewertet. Untersuchungen der Experton Group [1] belegen, dass nur eine Minderheit deutscher Unternehmen tatsächlich gemäß der oben skizzierten Best-Practices vorgeht. Nur 13 Prozent der Befragten haben z.B. tatsächlich eine Funktion des CISO. Deutlich weniger als jedes dritte Unternehmen hat einen Sicherheitsausschuss. Damit gibt es vielfach keine Funktion oder Institution im Unternehmen, die die Schnittstellenfunktionen zwischen IT, Management und den Geschäftsbereichen wahrnimmt. Die Ausrichtung der IT-Sicherheitsmaßnahmen an geschäftlichen und regulatorischen Anforderungen wird damit unwahrscheinlich, ebenso wie die Verknüpfung von IT- mit Business-Risiken.

Nicht selten gibt es zwar einen CISO, dieser berichtet aber an den CIO. Die Folge: die Maßnahmen für Informationssicherheit werden den Sach- und Budgetzwängen im IT-Bereich unterworfen. Damit können einige prinzipiell erforderliche Sicherheitsmaßnahmen nicht oder nur halbherzig umgesetzt werden. Ebenfalls kritisch zu bewerten ist die Situation eines CISO, der zwar außerhalb des IT-Bereichs angesiedelt ist, aber nur die Rolle eines Projektleiters einnimmt, ohne dass er starken Rückhalt durch den CEO bzw. die Geschäftsführung erhält. In dieser Situation wird es der CISO schwer haben, sich mit seinen Anliegen durchzusetzen.

## **4. Spezifische Rahmenbedingungen im Mittelstand**

Die zuvor beschriebenen Best-Practices eignen sich primär für Großunternehmen und den gehobenen Mittelstand sowie im Einzelfall auch für kleinere Mittelständler mit sehr hohen Sicherheitsanforderungen. In kleinen und mittelständischen Unternehmen mit weniger als 1000 Mitarbeitern können die skizzierten

Rollen nicht einfach auf dedizierte Vollzeitkräfte übertragen werden, bedingt vor allem durch die sehr beschränkten Ressourcen.

Dennoch kann sich auch ein mittelständisches Unternehmen an dem Rollenmodell orientieren. Die Rolle des CISO kann beispielsweise in Personalunion mit dem Personal- oder IT-Leiter wahrgenommen werden. In jedem Fall ist aber sicherzustellen, dass der betreffende Mitarbeiter ein festes Zeitkontingent für das Ausfüllen seiner Rolle als CISO erhält. Auch ist ein direkter Austausch mit der Geschäftsführung und den einzelnen Geschäftsbereichen sicherzustellen, sei es institutionalisiert oder informell. Von einer Personalunion von CISO und Datenschutzbeauftragtem sei abgeraten, denn letzterer soll ja die Wirksamkeit der durch den CISO oder auch IT-Verantwortlichen aufgesetzten Datenschutzmaßnahmen unabhängig prüfen.

## 5. Zusammenfassung

Das Informationssicherheitsniveau im Unternehmen hängt maßgeblich davon ab, wie gut die Verantwortlichkeiten und Prozesse für Informationssicherheit organisiert sind. Gut aufgestellte Unternehmen weisen die fachliche Verantwortung einem Chief Information Security Officer (CISO) zu, der außerhalb des IT-Bereichs steht und an den Chief Risk Manager oder direkt an ein Vorstandsmitglied berichtet. Auf diese Weise wird der Bezug zu den zu schützenden Werten auf der Geschäftsseite hergestellt, und der CISO hat mehr Kompetenzen, um seine Forderungen innerhalb und außerhalb des IT-Bereichs durchzusetzen.

Der CISO sorgt außerdem für eine multilaterale Kommunikation in Sachen Informationssicherheit. Über einen Sicherheitsausschuss (Security Steering Committee) kann dies institutionalisiert werden. Dadurch werden kontinuierlich Veränderungen bei den Sicherheitsanforderungen aus verschiedenen Unternehmensbereichen erfasst. Außerdem wächst das Verständnis und Bewusstsein für Informationssicherheit bei den Entscheidungsträgern im Unternehmen.

## 6. Literatur

- [1] Experton Group: Informationssicherheit im Spannungsfeld zwischen Technologie und Geschäftszielen - Status Quo und Trends in Deutschland – 2009+, Febr. 2009

---

© 2009 Eberhard von Faber und Friedrich–L. Holl, Brandenburg an der Havel, alle Rechte vorbehalten. Verwertung ist nur mit vollständiger Quellenangabe und unter Angabe der Bezugsquelle erlaubt. Reproduktion und anderweitige Wiedergabe des Dokumentes bedarf darüber hinaus der ausdrücklichen Genehmigung der Rechteinhaber.

---

**Titel:** The Bulletin Security Management  
**Herausgeber:** Eberhard von Faber und Friedrich–L. Holl

**ISSN:** 1869-2125  
**Bezugsquelle:** [www.security-management.de](http://www.security-management.de)

**Kontakt:**



Prof. Dr. Eberhard von Faber und  
Prof. Dr. Friedrich Lothar Holl  
Fachhochschule Brandenburg  
Fachbereich Wirtschaft  
Studiengang Security-Management  
Magdeburger Str. 50, 14770 Brandenburg

**Unterstützt von:**



Infos und Kontakt: [www.t-systems.de/ict-security](http://www.t-systems.de/ict-security)