

Risiko und Haftung von IT-Sicherheitsbeauftragten

Security Zone vom 22. September 2010

Ursula Sury, Rechtsanwältin

Probleme des SIBE

Der Sicherheitsbeauftragte/SIBE sieht verschiedene Probleme, die dringend gelöst werden müssten. Wie

- es sind weniger Lizenzen gelöst als verwendet werden.
- es bräuchte mehr und andere IT um Sicherheitsprobleme zu lösen.
- das Back-up-Prozedere ist ungenügend.
- etc.

Und jetzt?

- Der SIBE beantragt beim VR/Board zusätzliche Ressourcen um diese Probleme fach- und sachgerecht lösen zu können.
- Die benötigten Ressourcen werden nicht bewilligt.

Macht sich der SIBE straf- oder zivilrechtlich mitverantwortlich für

- Datenschutzverletzungen
- Urheberrechtsverletzungen
- Persönlichkeitsverletzungen
- Strafrechtliches Verhalten von Mitarbeitenden wie Erwerb und halten Kinderpornographie, Brutalos, rassistische Inhalte

?

OR 321e

Haftung des Arbeitnehmers

¹ Der Arbeitnehmer ist für den Schaden verantwortlich, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt.

² Das Mass der Sorgfalt, für die der Arbeitnehmer einzustehen hat, bestimmt sich nach dem **einzelnen Arbeitsverhältnis**, unter Berücksichtigung des Berufsrisikos, des **Bildungsgrades** oder der **Fachkenntnisse**, die zu der Arbeit verlangt werden, sowie der Fähigkeiten und Eigenschaften des Arbeitnehmers, **die der Arbeitgeber gekannt hat oder hätte kennen sollen.**

Zivilrechtliche Haftungsvoraussetzungen

- Schaden
 - +
 - Widerrechtlichkeit
 - +
 - Adäquater Kausalzusammenhang
 - +
 - Verschulden

StGB 143

Unbefugte Datenbeschaffung

¹ Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

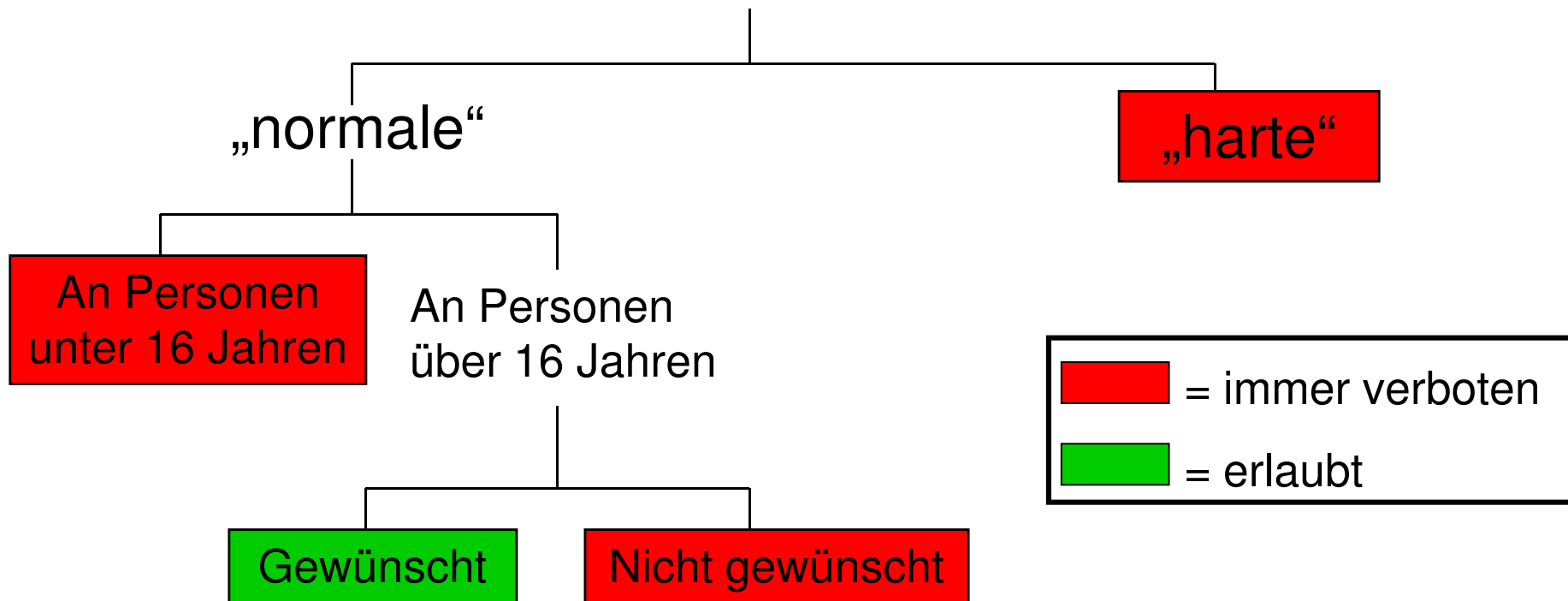
² Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

StGB 143^{bis}

Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Art. 197 StGB Pornografie



Ausnahme: Schutzwürdige Kulturelle oder wissenschaftlichen Wert

Voraussetzungen der Strafbarkeit

Tatbestandmässigkeit

Entspricht die Tat der vom Gesetz umschriebenen Situation?

+

Rechtswidrigkeit

Liegt ein Rechtfertigungsgrund vor oder nicht?

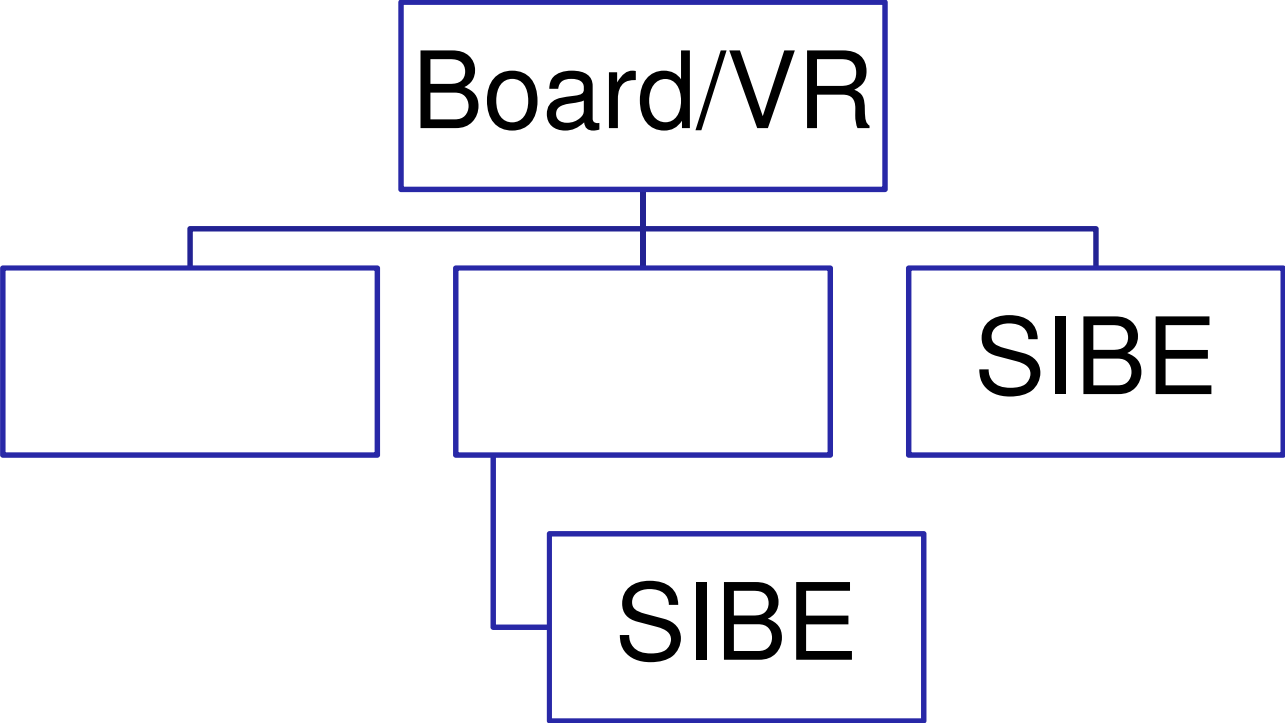
+

Schuldhaftigkeit

Wurde die Tat vorsätzlich begangen oder in Kauf genommen?

Delegation/Übertragung von Haftung und Verschulden

→ Kann ich mich so organisieren, dass ich gegenüber jedem belegen kann, dass ich keinen Rechtsatz/kein Gesetz verletzt habe?



Checkliste Haftpflicht

Schaden

Der ist sicher entstanden.

Rechtswidrigkeit d.h. Vertragsverletzung

Dies kann der SIBE belegen,
dass er sie nicht begangen hat.

Adäquater Kausalzusammenhang

Nicht mehr zu prüfen

Verschuldung

Nicht mehr zu prüfen

→ Folglich ist der SIBE zivil- d.h. haftpflichtrechtlich
nicht verantwortlich.

Abwehr der zivilrechtlicher Haftung

- Optimale Erfüllung zu der vertraglichen Verpflichtung.
- Dort wo die vertraglichen Verpflichtungen nicht erfüllt werden können wegen mangelnden Ressourcen, müssen diese begründet bei den zuständigen Personen eingefordert werden.
- Die zuständigen Personen müssen klar und eindeutig auf die Auswirkungen der Nichtgewährung der Ressourcen hingewiesen werden.

→ 321e OR ist für SIBE kein Problem

Abwehr der strafrechtlicher Verantwortlichkeit

Strafbarkeit betrifft immer einen bestimmten Täter, i.d.R. eine natürliche Person.

Kann der SIBE belegen, dass ihm der im Gesetz umschriebene Tatbestand nicht zugeschrieben werden kann?

- Tatbestandsmässigkeit wird gegeben sein.
- Rechtswidrigkeit wird gegeben sein, da ein Rechtfertigungsgrund fehlt.
- Schuldhaftigkeit, Vorsatz oder in Kauf nehmen? Hier kann der SIBE wiederum mit dem Beleg, dass er rechtzeitig und sehr klar die zuständigen Personen auf die Probleme hingewiesen hat, seine Schuldlosigkeit beweisen und somit Straffreiheit erlangen.
- Strafrechtliche Verantwortung kann wahrscheinlich abgewehrt werden

Verantwortlichkeit des Verwaltungsrates und des Managements

- Persönlich
- Solidarisch
- Nicht delegierbar
- Risk & Compliance
- IKS (Internes Kontrollsystem) und IT-Security

OR 716a

Unübertragbare Aufgaben

¹ Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die **Oberleitung der Gesellschaft** und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;

OR 716a

Unübertragbare Aufgaben

4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. Die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die **Befolgung der Gesetze**, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes² sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;

OR neu 728a

Aufgaben der Revisionsstelle

a. Gegenstand und Umfang der Prüfung

1 Die Revisionsstelle prüft, ob:

1. die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;
2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;
3. **ein internes Kontrollsystem existiert.**

2 Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.

3 Die Geschäftsführung des Verwaltungsrats ist nicht Gegenstand der Prüfung durch die Revisionsstelle.

OR neu 728b

Revisionsbericht

- 1 Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision.**
- 2 Die Revisionsstelle erstattet der Generalversammlung schriftlich einen zusammenfassenden Bericht über das Ergebnis der Revision. Dieser Bericht enthält:
 1. eine Stellungnahme zum Ergebnis der Prüfung;
 2. Angaben zur Unabhängigkeit;
 3. Angaben zu der Person, welche die Revision geleitet hat, und zu deren fachlicher Befähigung;
 4. eine Empfehlung, ob die Jahresrechnung und die Konzernrechnung mit oder ohne Einschränkung zu genehmigen oder zurückzuweisen ist.
- 3 Beide Berichte müssen von der Person unterzeichnet werden, die die Revision geleitet hat.

OR neu 662

Geschäftsbericht

I. Im Allgemeinen

1. Inhalt

- ¹ Der **Verwaltungsrat erstellt** für jedes Geschäftsjahr einen Geschäftsbericht, der sich aus der **Jahresrechnung**, dem Jahresbericht und einer Konzernrechnung zusammensetzt, soweit das Gesetz eine solche verlangt.
- ² **Die Jahresrechnung besteht aus** der Erfolgsrechnung, der Bilanz und **dem Anhang**.

OR neu 663b

Anhang

IV. Anhang 1. Im Allgemeinen

Der Anhang enthält:

- 12. Angaben über die Durchführung einer Risikobeurteilung;**

Die Bestimmungen über IKS und Risikobeurteilung gelten auch für

- die GmbH (Art. 801 und 818 OR)
- die Kommandit AG (Art. 764 Abs. 2 OR)
- die Genossenschaft (Art. 906 und Art. 908 OR)
- den revisionspflichtigen Verein (Art. 69b Abs. 3 ZGB)
- die Stiftung (Art. 83a Abs. 2 und 83b Abs. 3 ZGB)

Aufgaben des Verwaltungsrates → IKS

Alter Wein in einem zusätzlichen neuen Schlauch

- Führungsverantwortung impliziert Kontrolle, diese muss systematisch durchgeführt werden.
- Risikomanagement impliziert auch regelmässige Kontrolle, systematisiert werden kann diese mit einem IKS.
- Die Revision prüft, ob ein IKS besteht.



Auszug aus einer Präsentation der KPMG von 2007

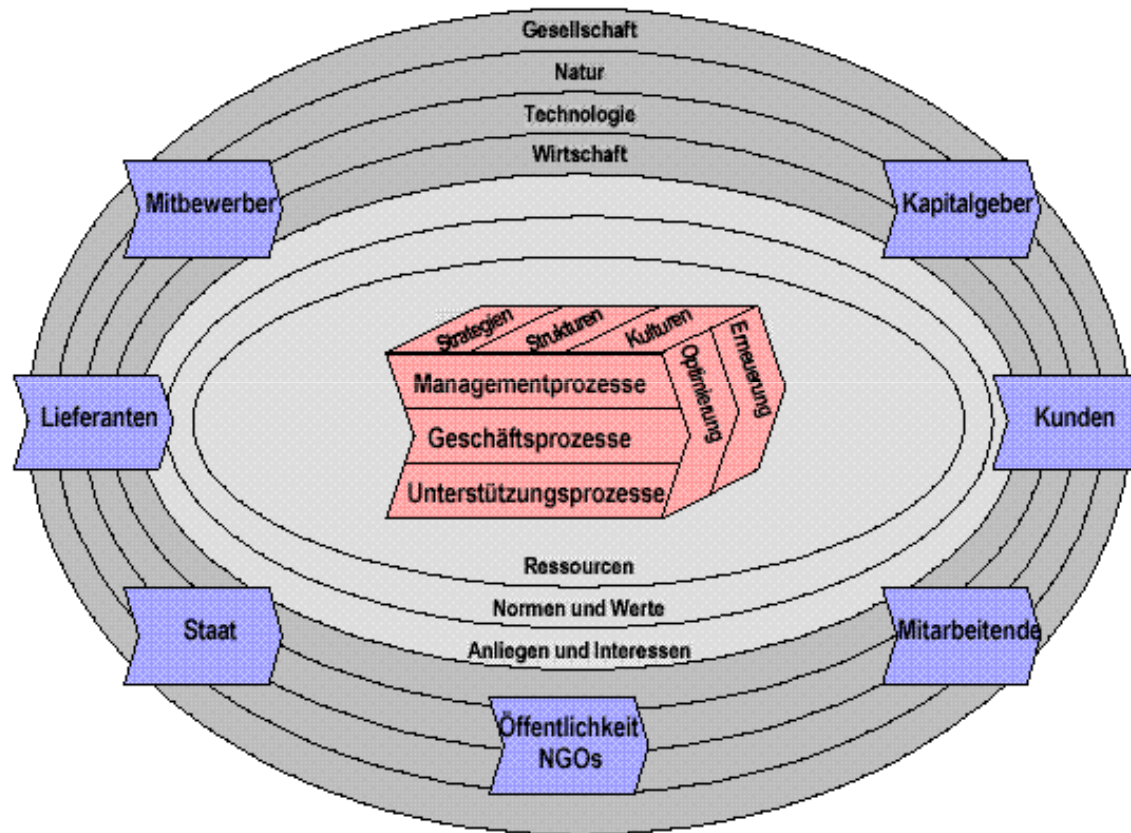
Risikobeurteilung und IKS → Auswirkungen auf die Informationssicherheit

- IKS wird eher als umfassende und breite Verantwortung des Verwaltungsrates verstanden, der Blickwinkel wird auf das Unternehmen in seiner Gesamtheit gelegt, da es gemäss Gesetz selbständiger Prüfungsgegenstand der Revision ist.
- Die Risikobeurteilung wird eher als ein Element des IKS verstanden, da es nur in einem unter mehreren Anhängen zu erwähnen ist.

Auswirkungen auf die Informationssicherheit

- Der Verwaltungsrat ist für die **Oberleitung** der Gesellschaft, der damit verbundenen und dafür notwendigen Organisation in sämtlichen unternehmerischen Bereichen verantwortlich
- **Führungsverantwortung** impliziert Auswahl, Instruktion und **Kontrolle** von Personen im Hinblick auf optimale Erreichung unternehmerischer Ziele
- Sorgfältige Unternehmensführung impliziert, dass Gesetze eingehalten und sämtliche **unternehmerischen Risiken minimiert** werden
- Damit unternehmerische Risiken minimiert werden können, müssen sie erkannt (verstanden!) und bewertet werden

St. Galler Management Konzept: Die Unternehmung als dynamisches System



Auswirkungen auf die Informationssicherheit

- Sicher funktionierende **IT** liefert die für die Geschäftsführung notwendigen **Managementinformationen**
- Sicher funktionierende **IT** ermöglicht in vielen Betrieben erst die Erfüllung/Erstellung des **Geschäftsprozesses**
- Sicher funktionierende **IT** ist das zentrale Element jedes unternehmerischen **Unterstützungsprozesses**

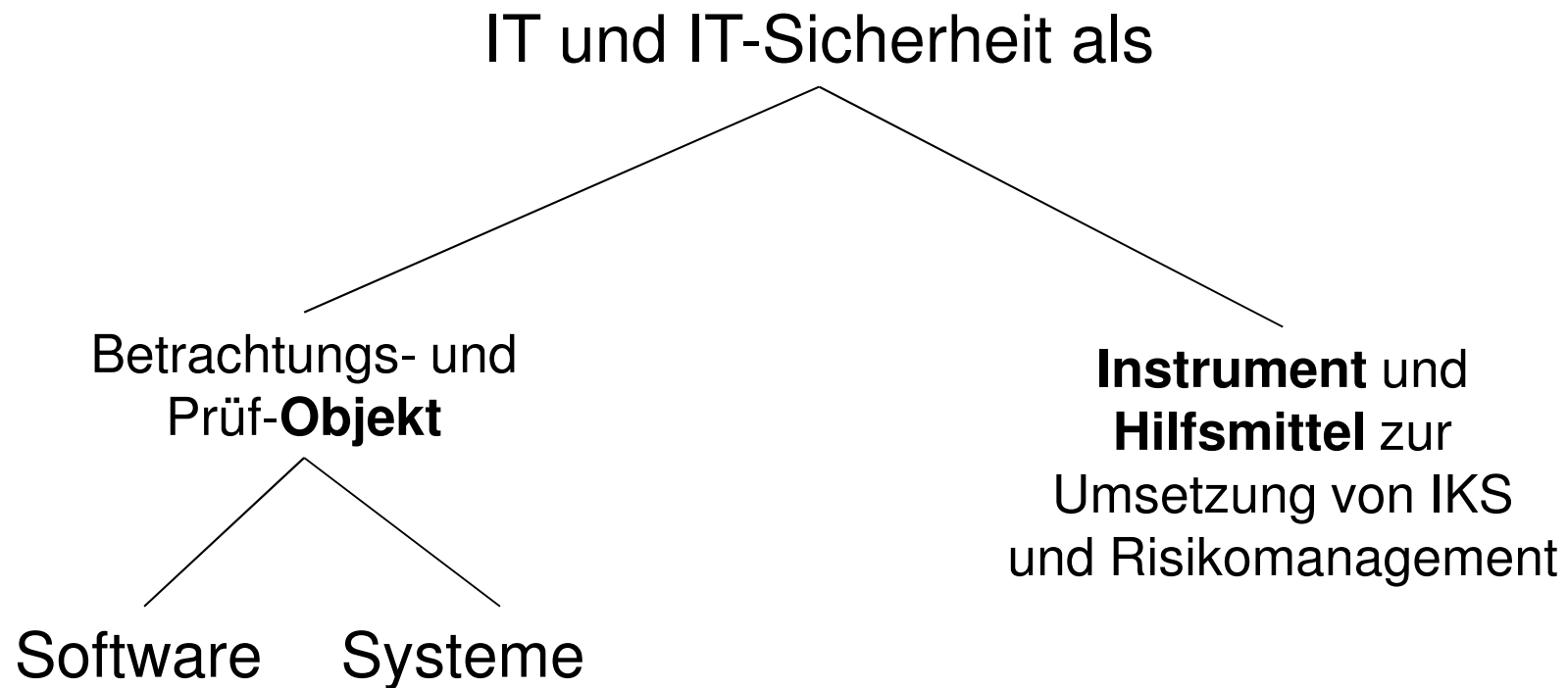
Management-, Geschäfts- und Unterstützungsprozess

Managementprozess IT-Sicherheit IT-Governance
Geschäftsprozess IT-Sicherheit IT-Governance
Unterstützungsprozess IT-Sicherheit IT-Governance

IKS, Risikobeurteilung und Informationssicherheit

- Die (in der Literatur vielfach diskutierten und bekannten) **Risiken der IT und insbesondere der IT-Sicherheit** müssen folglich im Rahmen einer Risikobeurteilung und eines IKS **festgestellt** (verstanden!) und bewertet werden
- Es sind **Massnahmen zur Minimierung der Risiken** aufzuzeigen oder es ist zu erläutern, warum man mit welchen Risiken bewusst leben kann

IKS, Risikobeurteilung und Informationssicherheit



Sicherheitsanforderungen an IT-Produkte als solche → Objekte

IT-Produkte/Software muss inhaltlich so angelegt sein
dass sie:

- kein Risiko bilden
- keine Falses generieren (z. B. falsche Managementinformati-onen, falsche Aussagen in der Jahresrechnung o. ä.)
- korrekte Managementinformationen liefern
- korrekten Geschäftserstellungoutput liefern
- keine Gesetze verletzen
- Integrität
- etc.

Risiken beim Einsatz von ganzen IT-Systemen → Objekt

- Ausfallrisiken
- zu weit gehendes Monitoring (Datenschutzverletzung!)
- unsichere Transaktionen
- nicht beweisbare Transaktionen
- falsche Zustellungen
- Datenqualität
- Datensicherheit
- Risiken bei Systemänderungen
- Risiken bei Systemunterhalt
- wie wird die IT eingesetzt?
- wie wird auf Probleme mit IT-Systemen durch die Unternehmen resp. das Management reagiert?
- etc.

Informatik und Informatiksicherheit als Instrumente und Hilfsmittel des IKS

- IT und die IT-Sicherheit von der Unternehmung selber regelmässig überprüft
- Zugriffsregelungen und Authentisierungen
- Verschlüsselungen
- Monitoring
- Anonymisierung
- Pseudonymisierung
- etc.

Zivilrechtliche Haftung Board/VR

- Der Verwaltungsrat ist zu **sorgfältiger Geschäftsführung** persönlich verpflichtet
- sorgfältige Geschäftsführung impliziert **Kontrolle**
- die Durchführung von systematischen Kontrollen muss im Rahmen einer **Risikobeurteilung** und eines **IKS** nachgewiesen werden
- welche konkreten Anforderungen der Gesetzgeber an die Risikobeurteilung und ans IKS stellt ist noch weitgehend unklar
- was die Revisionsstelle alles prüft resp. prüfen muss, ist noch weitgehend unklar, Hinweise ergibt der PS890
- IT und IT-Sicherheit sind wesentliche und **essentielle Elemente des Management-, Geschäfts- und Unterstützungsprozesses** einer Unternehmung und sind somit mit den entsprechenden Risiken behaftet
- **IT und IT-Sicherheit** bildet sowohl betreffend der verwendeten Produkte als auch ganzer Systeme und Verfahren **Bestandteil einer Risikobeurteilung und eines IKS**

Strafrechtliche Verantwortung Board/VR

Tatbestandsmässigkeit	Gegeben
Rechtswidrigkeit	Gegeben
Schuldhaftigkeit	Gegeben, wenn er bei Kenntnis der Situation oder wenn er aufgrund der Sorgfaltspflicht die Situation hätte gekannt müssen.

Achtung!

Haftung für Inhalte und für Links!

Man ist auch dafür verantwortlich, dass die Links, die man setzt, korrekt sind. Probleme sind

- Insb. Urheberrechtsverletzungen
- Allgemeine Straftatbestände

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen

www.dieadvokatur.ch

Weiterbildungen (auch IT-Recht) www.hslu.ch

Ursula Sury

Rechtsanwältin, Prof. an der Hochschule Luzern

Die Advokatur Sury GmbH

Alpenquai 4

6005 Luzern