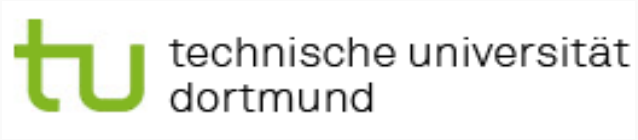


STUDIE ZU IT-RISIKOBEWERTUNGEN IN DER PRAXIS

Stefan Taubenberger und Prof. Jan Jürjens, 22. September 2011

Ziele der Studie

Konfirmative und explorative Studie mit folgenden Fragestellungen

- Welche Kriterien und Objekte werden in der IT-Risikobewertung verwendet, und wie?
- Sind Daten wie Prozessmodelle, Sicherheitsanforderungen und Datenklassifikation in der Praxis vorhanden?
- Wie werden Prozessmodelle und Sicherheitsanforderungen genutzt?
- Führt die Bewertung von Risiken anhand Sicherheitsanforderungen zu genaueren Ergebnissen?
- Werden Sicherheitsanforderungen genutzt und Kontrollen systematisch überprüft?

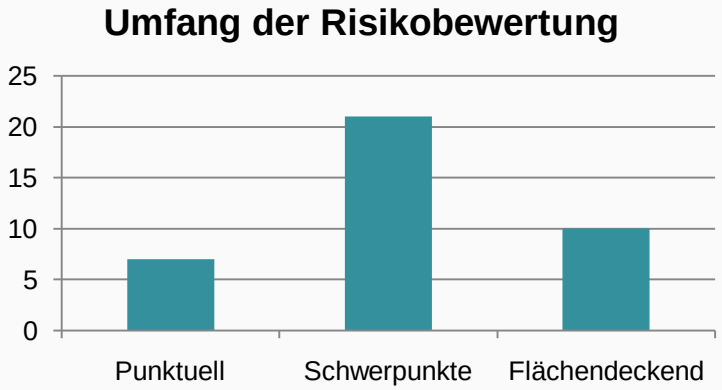
Der Fokus der Studie befasste sich mit Kriterien in der IT-Risikobewertung und die Nutzung von Sicherheitsanforderungen.

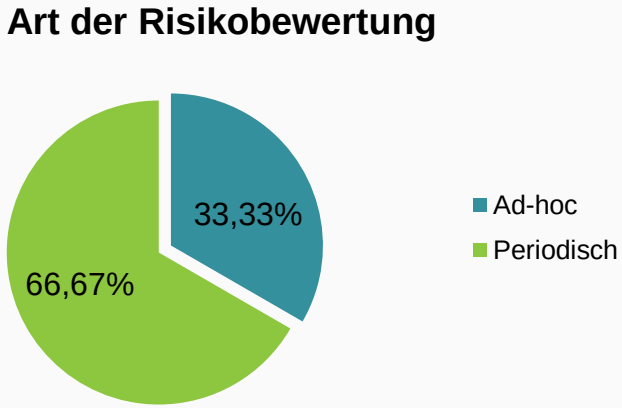
Ablauf und Inhalte der Studie

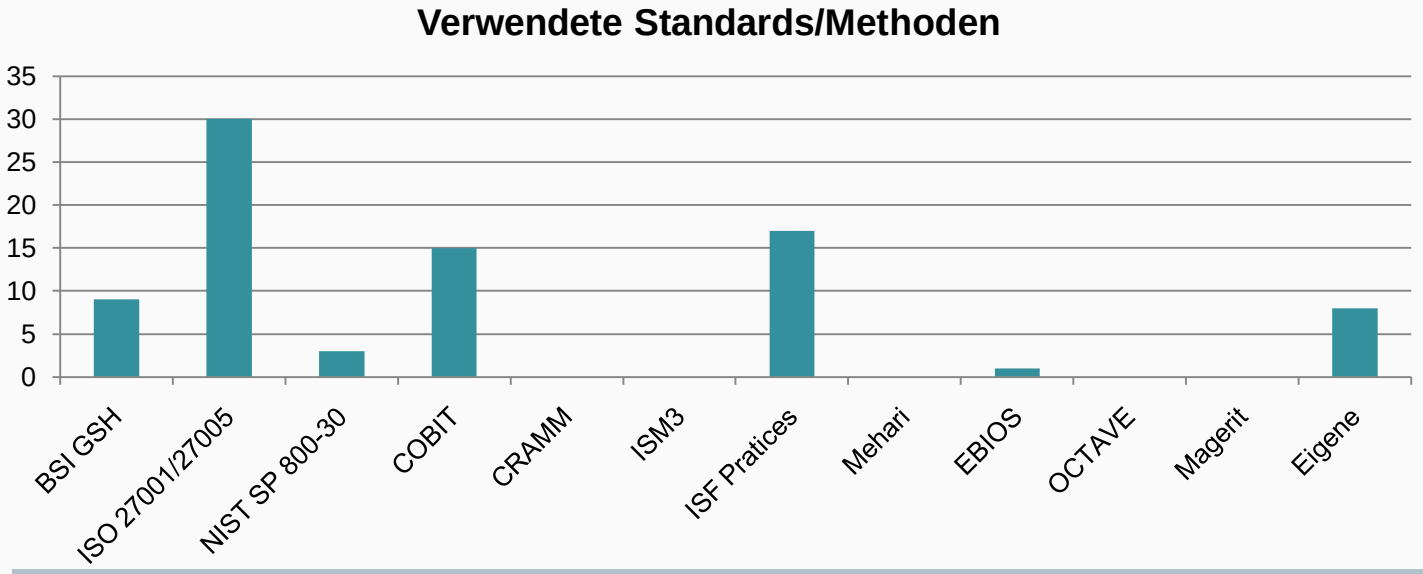
- 55 Teilnehmer an der Studie, die unter Aufsicht in einem geschlossenen Raum stattfand. Teilnehmer hatten ca. 30 Minuten Zeit zur Bearbeitung des Fragebogens.
- 3 Teile in der Studie
  - Teil 1 - Fragen zur IT-Risikobewertung, 45 auswertbare Antworten.
  - Teil 2 - Geschäftsprozessmodelle und Sicherheitsanforderungen, 46 auswertbare Antw.
  - Teil 3 – Risikobewertung anhand eines Beispiels
    - Bsp. A – Risikosituation, 12 auswertbare Antworten
    - Bsp. B – Risikosituation und Prozessmodell, 13 auswertbare Antworten
    - Bsp. C – Risikosituation, Prozessmodell und Sicherheitsanforderungen, 11 auswertbare Antworten

IT Sicherheitsexperten aus der Praxis wurden befragt zur IT-Risikobewertung und Verfügbarkeit von Geschäftsprozessmodellen. Eine beispielhafte Risikoanalyse wurde von den Teilnehmern durchgeführt.

Teil 1: IT Risikobewertung - Ergebnisse der Studie

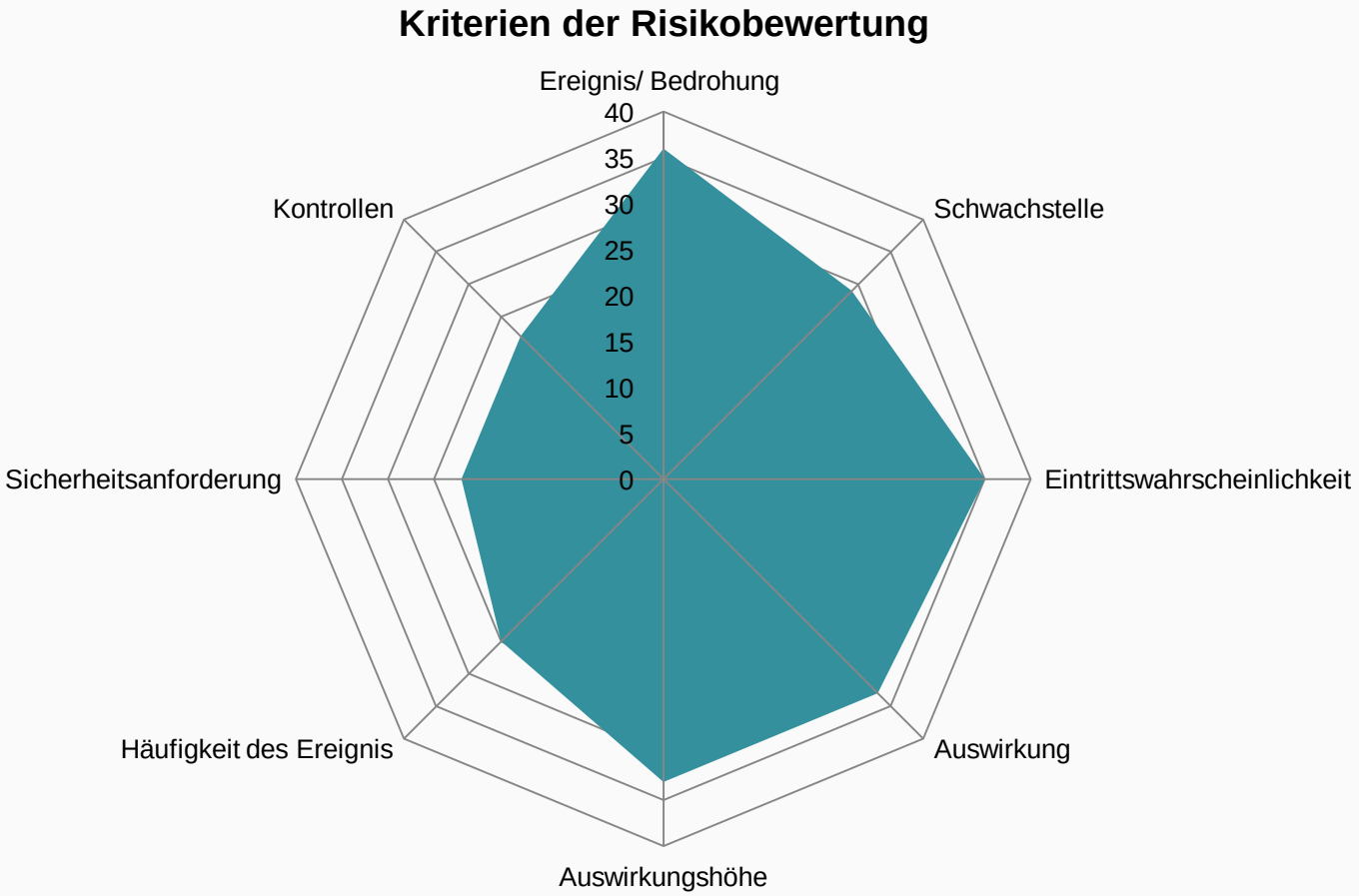






IT Risikobewertungen werden perodisch mit Schwerpunkten durchgeführt. Hauptsächlich werden Best-Practice-Methoden verwendet.

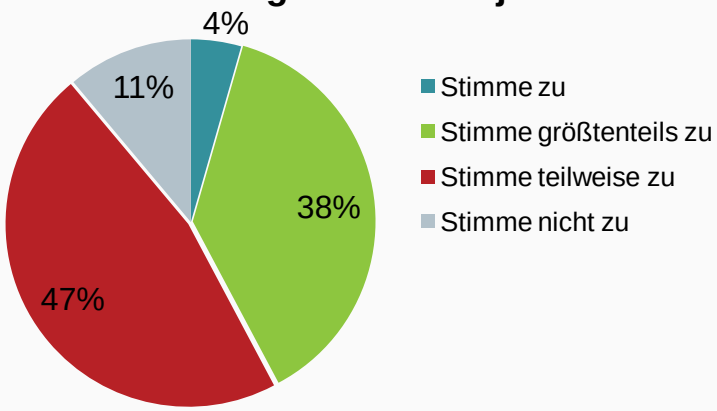
Teil 1: IT Risikobewertung - Ergebnisse der Studie



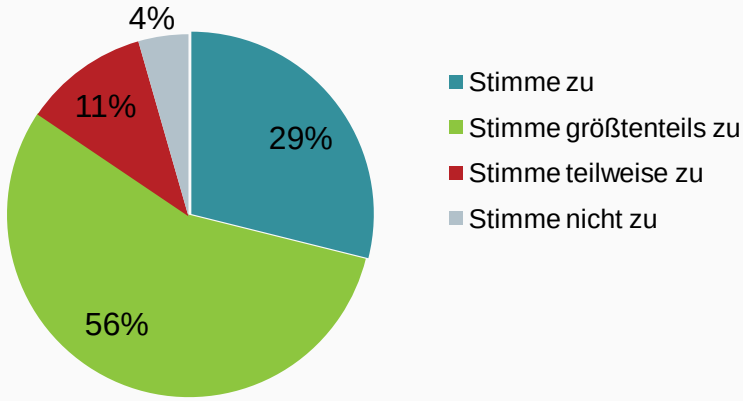
Häufigkeiten, Sicherheitsanforderungen und Kontrollen werden nur von einem kleinen Teil der Teilnehmer verwendet.

Teil 1: IT Risikobewertung - Ergebnisse der Studie

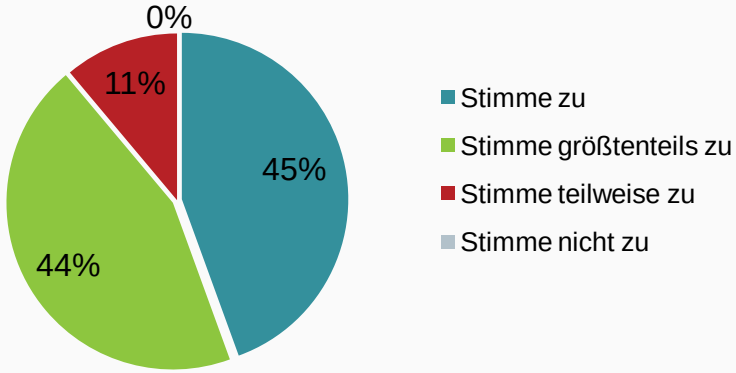
Risikobewertungen sind subjektiv



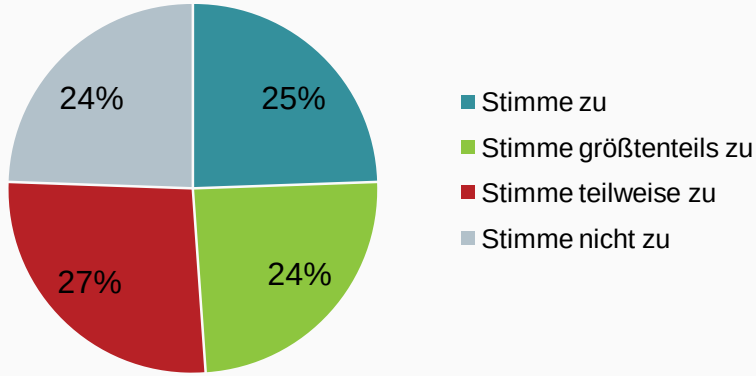
Risikobewertungen sind beeinflusst



Umsetzung von Sicherheitsmaßnahmen ist beeinflusst

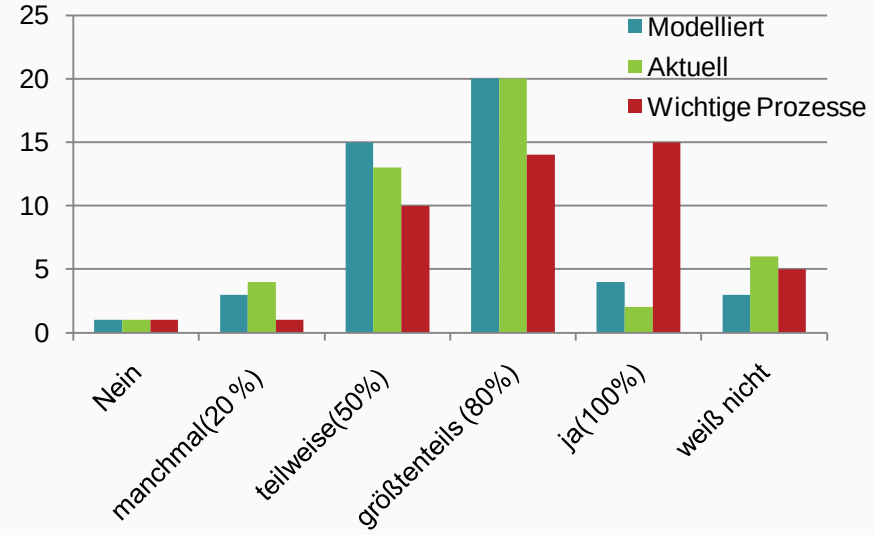


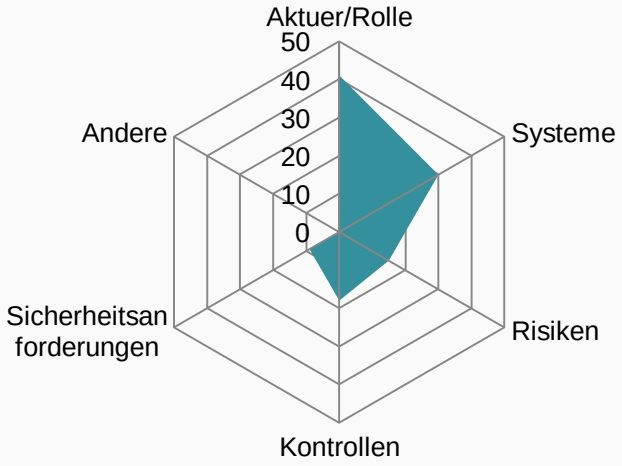
Sicherheitsrichtlinien werden angepasst

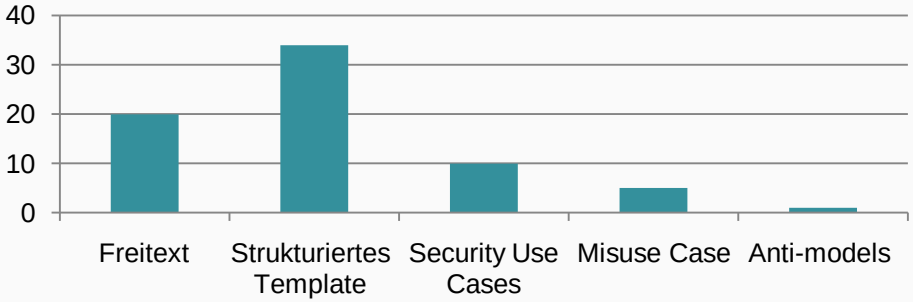


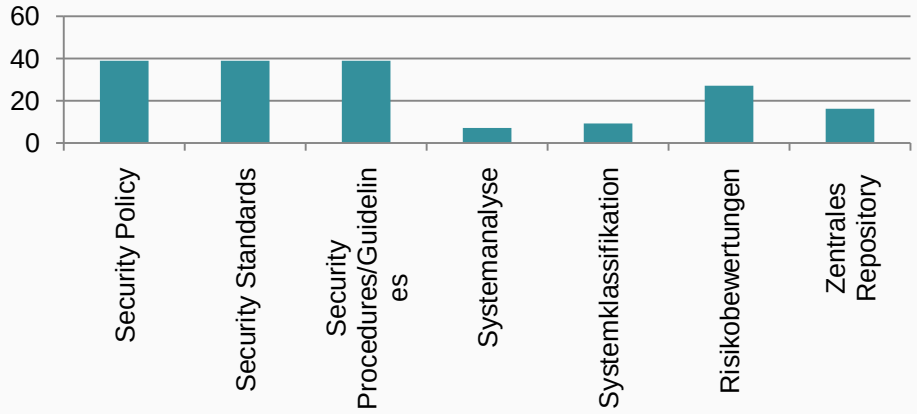
Risikobewertungen sowie die Umsetzung von Sicherheitsmaßnahmen ist beeinflusst durch Erfahrungen, Medien sowie Kostenzielen.

Teil 2: Geschäftsprozessmodelle und Sicherheitsanforderungen - Ergebnisse der Studie





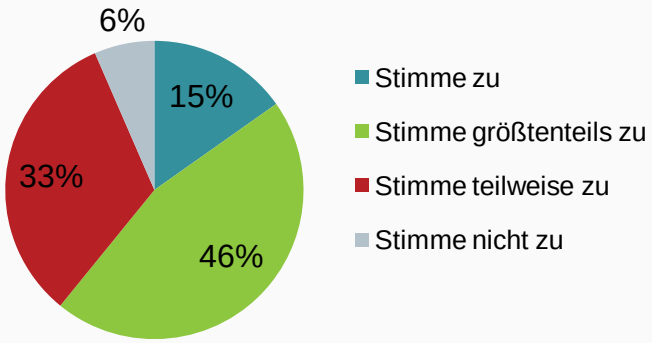




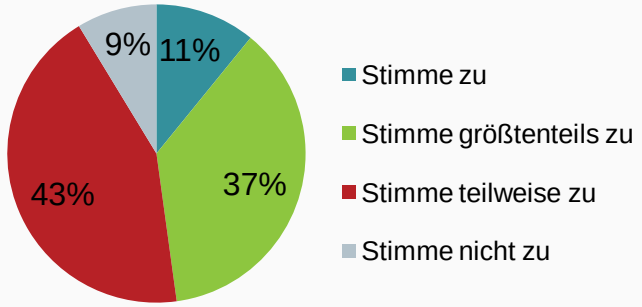
Geschäftsprozessmodell sind größtenteils modelliert und aktuell, sowie Akteure und Systeme modelliert. Sicherheitsanforderungen werden mit strukurierten Templates z.B. in Security-Policies, -Standards dokumentiert.

Teil 2: Geschäftsprozessmodelle und Sicherheitsanforderungen - Ergebnisse der Studie

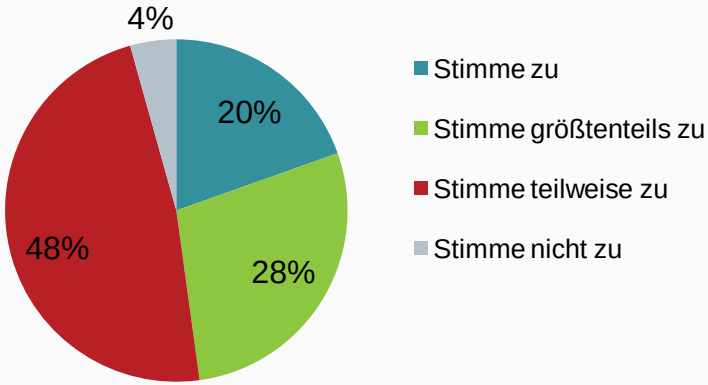
IT Prozess-Maturity



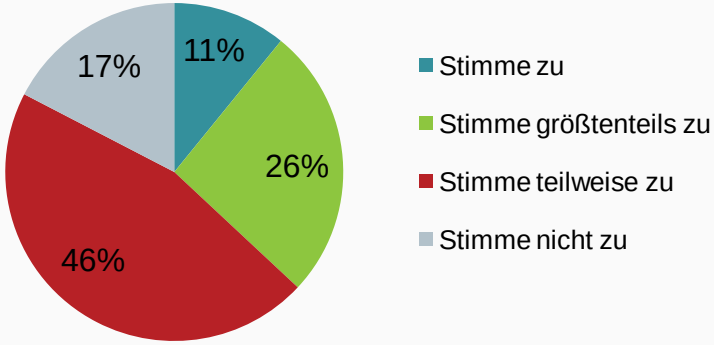
IT Prozess-Performance



Überprüfung der Datensicherheit mit SR



Wir messen die Sicherheit von Daten



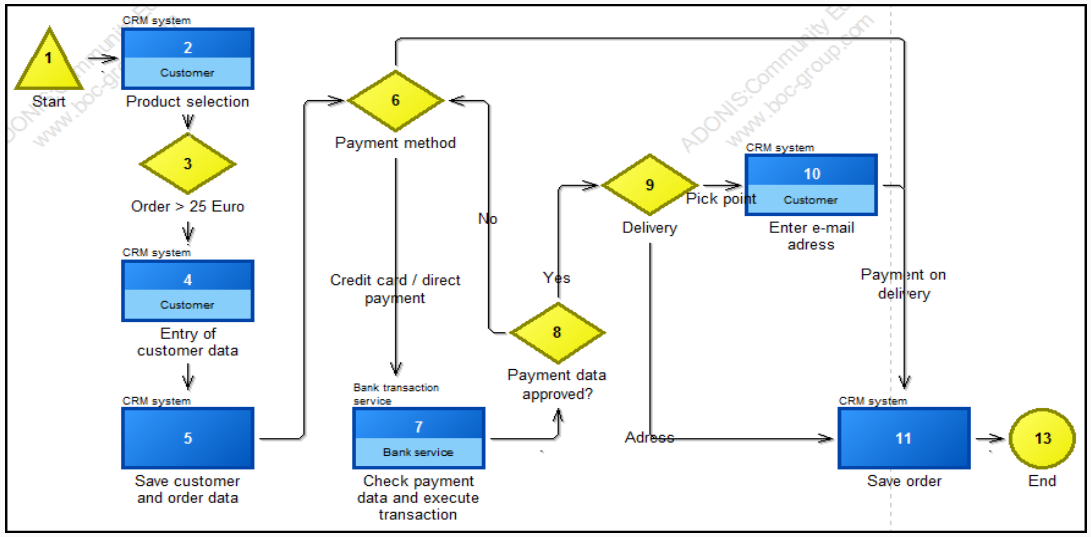
Die Bewertung von Maturity und Performance von IT-Prozessen könnte zu beständigeren Risikobewertungen führen. Die Datensicherheit wird nur zum Teil überprüft und gemessen.

Teil 3: Risikoanalyse am Beispiel - Ergebnisse der Studie

Risikosituation (A,B,C *)

Ein Unternehmen verkauft alle Waren über einen Online-Shop. Siehe dazu das folgende Prozessmodell. Pro Tag werden ca. 1000 Bestellungen abgewickelt und nur Bestellungen die höher als 25 Euro sind werden in dem Online CRM System gespeichert und bearbeitet. Möchte der Kunde mit Kreditkarte oder per Banküberweisung bezahlen, werden die Daten an eine Bank weitergeleitet, die die Bezahlung übernimmt. Das Online System ist wichtig für das Unternehmen, da alle Umsätze über das Online Portal erzeugt werden. Im Rahmen einer Analyse wurde festgestellt, dass über Eingabefelder im Online Bestellsystem (CRM System) Datenbankinhalte geändert werden können (Prozessschritt 4). Außerdem werden Kundendaten sowie Zahlungsdaten nicht verschlüsselt übertragen (Prozessschritt 5,6 und 7). Alle Mitarbeiter des Bestellprozesses haben lesenden Zugang zu den Bestelldaten im CRM System. Das CRM System war in den letzen 10 Tagen 2 mal für 1 Stunde nicht verfügbar, aufgrund eines Systemausfalls der durch Wartungsarbeiten verursacht war.

Prozessmodell (B,C *)



Sicherheitsanforderungen (C *)

Folgende Sicherheitsanforderungen sind definiert: Der Geschäftsprozess „Bestellung“ ist als kritisch für den Betrieb eingestuft, es gilt für alle Kunden-, Bestell- und Zahlungsdaten: die Vertraulichkeit und Integrität der Daten muss sichergestellt sein und IT-Systeme sollten höchstens 15 Minuten pro Tag nicht verfügbar sein. Im Geschäftsprozess „Rechnung“ wurde festgelegt, dass nur Mitarbeiter des Rechnungswesen alle Bestelldaten einsehen dürfen. Gespeicherte Transaktionen (Bestelldaten) im Bestellprozess sind, nach der Speicherung der Bestellung, durch einen Mitarbeiter der Bestellung zu autorisieren und an den Prozess „Rechnung“ zu übermitteln.

* Der Indikator A,B,C bezeichnet, in welchen Beispielen der Studie welche Informationen vorhanden waren.

Unterschiedliche Informationen waren in dem Risikoanalysebeispiel gegeben.

Teil 3: Risikoanalyse am Beispiel - Ergebnisse der Studie

	Identifizierte Risiken in Prozent		
Definierte Risiken	**Beispiel A** Nur Risikosituation	**Beispiel B** Risikosituation + Prozessmodell	**Beispiel C** Alle Informationen
1.Data integrity (in Beispiel A, B and C)	100%	100%	73%
2. Data confidentiality (in Beispiel A, B und C)	67%	85%	91%
3. Process design - data confidentiality access control (nur Beispiel C)	8%	0%	45%
4. System availability (nur Beispiel C)	100%	85%	100%
5. Process design - authorization (nur Beispiel C)	0%	0%	20%
6. Other risks (in Beispiel A, B und C)	75%	77%	55%

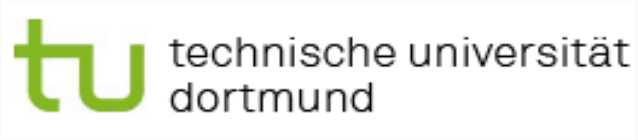
Informationen werden interpretiert und Annahmen getroffen. Die Risiko-bewertung ist genauer (Anzahl der Risken), je mehr Informationen vorhanden sind. Komplexe Sachverhalte können die korrekte Risikoidentifikation negativ beeinflussen.

Fazit der Studie

- Hauptsächlich werden Best-Practice Methoden und keine Risikobewertungsverfahren im engeren Sinne verwendet.
- Risikoergebnisse und der Bewertungsvorgang werden als nicht objektiv sowie beeinflusst durch verschiedene äußere Einflüsse wie Risikobewußtsein, Kostenziele oder Medien angesehen.
- Eine systematische Bewertung der Kontrollen für alle Assets wird nicht oder unzureichend vorgenommen.
- Die Studie hat bestätigt, dass Geschäftsprozessmodelle für kritische bzw. wichtige Prozesse eines Unternehmens in der Praxis vorhanden und diese auch aktuell sind.
- Das Thema Sicherheitsmonitoring und Sicherheitsmessung ist bei den meisten Unternehmen nicht sehr ausgeprägt.
- IT-Systeme und/oder Daten werden in Unternehemen nach Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert.
- Das Risikobewertungsbeispiel in der Studie zeigt, dass Risiken korrekter identifiziert werden, je mehr Informationen (wie z.B. Sicherheitsanforderungen) vorliegen.

Ausblick

- IT Risikobewertungsmethoden sollten besser mit dem Risikomanagement und Compliance-Aktivitäten verbunden werden und die Effektivität und Effizienz von Methoden gesteigert werden.
- Einbindung der Ergebnisse in das zentrale Risikomanagement, sowie auch die Bewertung von übergreifenden operationellen Risiken.
- Erweiterung der Datenbasis sowie Objektivierung des Bewertungsvorgangs. Bsp. Schadensvorfälle, -potentiale, Szenarios und Abhängigkeiten zwischen Assets, Prozessen und Schadensvorfällen.
- Kontinuierliches Monitoring, Überwachung und Messung von Sicherheit.
- Entwicklung von Methoden oder Werkzeuge für die Darstellung und Auswertung von komplexen Sachverhalten und wichtigen Informationen im Kontext der Risikoanalyse und –bewertung.



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt: http://jan.jurjens.de

Stefan Taubenberger und Prof. Jan Jürjens