Bundesamt
für Sicherheit in der
Informationstechnik

Grenzen des quantitativen Risikomanagements

SECMGT-Workshop "IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten"

Isabel Münch
IT-Grundschutz und Allianz für Cyber-Sicherheit

Agenda

- Risikomanagement-Standards
- Diskussionen in der ISO
- Risikoanalyse nach 100-3
- Qualitativ oder quantitativ

Risikomanagement

Unterschiedliche Ansätze, gemeinsames Ziel

- Entwicklungen in und um eine Institution beobachten und auf Gefährdungspotentiale untersuchen
- Gefährdungen und Sicherheitsvorfälle realistisch bewerten
- Risiken angemessen behandeln

Risikomanagement für viele Arten von Geschäftsprozessen und Aktivitäten

- Kategorien wie strategische, technologische, marktwirtschaftliche, operationelle, finanzielle, personelle, rechtliche und IT-Risiken

Risikomanagement-Standards

- Mehr als 50 verschiedene internationale Standards sowie unzählige nationale oder firmenspezifische Standards
- Unterschiedliche Branchen, unterschiedliche Ansätze und Techniken zur Risikobewertung
- Bestreben in der ISO, Begrifflichkeiten und Vorgehensweisen zu vereinheitlichen
- ISO 31000 soll maßgeblich werden

Was ist ein Risiko?

- "risk = effect of uncertainty on objectives" [ISO Guide 73:2009, definition 1.1]

- Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. [IT-Grundschutz]

- Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.
- Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

ISO 31010

Table A.1 – Applicability of tools used for risk assessment

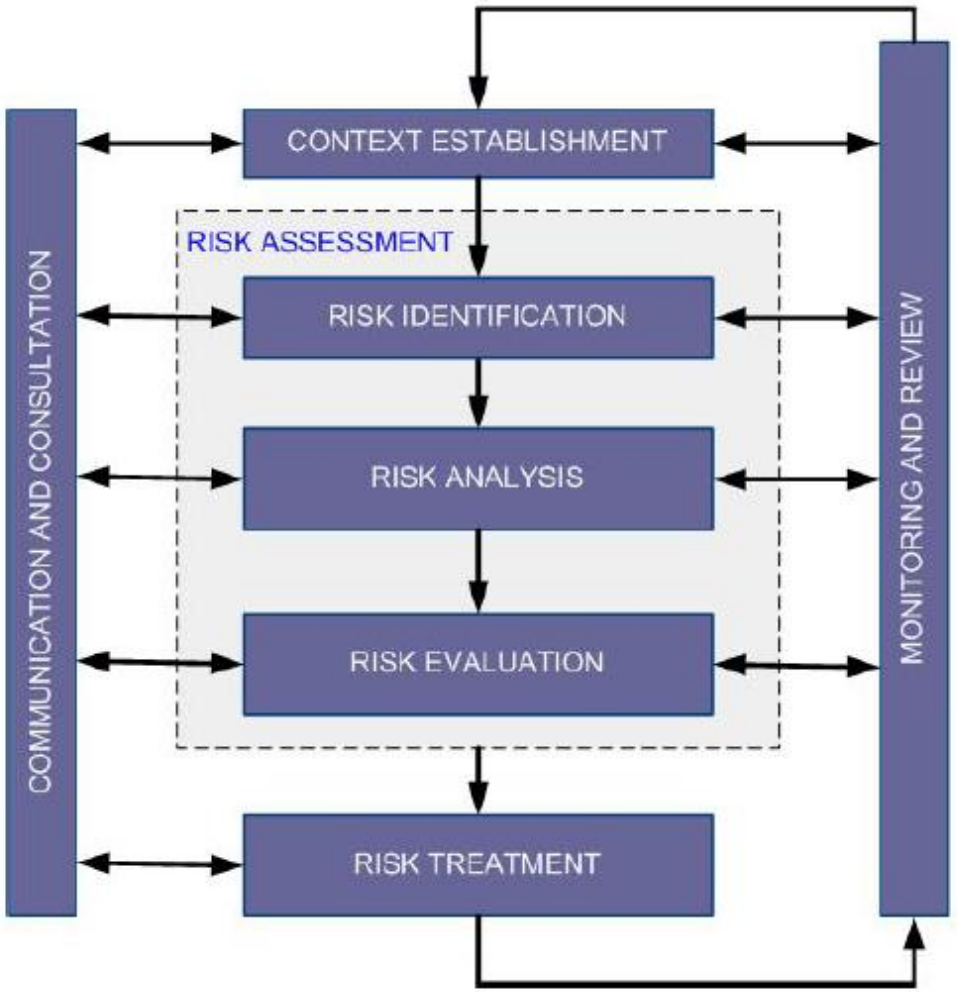
Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	S				
Root cause analysis	NA	S				
Failure mode effect analysis	SA	S				
Fault tree analysis	A	N				

Lange Tabelle verschiedener Risikoanalyse Methoden

Quelle: ISO 31010:2009

ISO 31000

Risk management process as specified in ISO 31000



Quelle: ISO 27005:2011

ISO 27005:2011
Status Überarbeitung

- ISO SC 27 hatte die Aufgabe, 27005:2011 an die Revision der 27001:2013 anzupassen
- Auf der letzten ISO-Sitzung im April 2016 wurde diese Anpassung gestoppt
  - Scope ("Projektauftrag" der ISO) zu eng definiert, grundlegende Überarbeitung notwendig
  - Harmonisierung mit
    - ISO 20000 (Service Management)
    - ISO 31000 (Risk Management)
    - ISO 55000 (Asset Management)
  - ISO 31000 und Guide 73 werden aktuell parallel überarbeitet, diese bilden die Basis für die ISO/IEC 27005

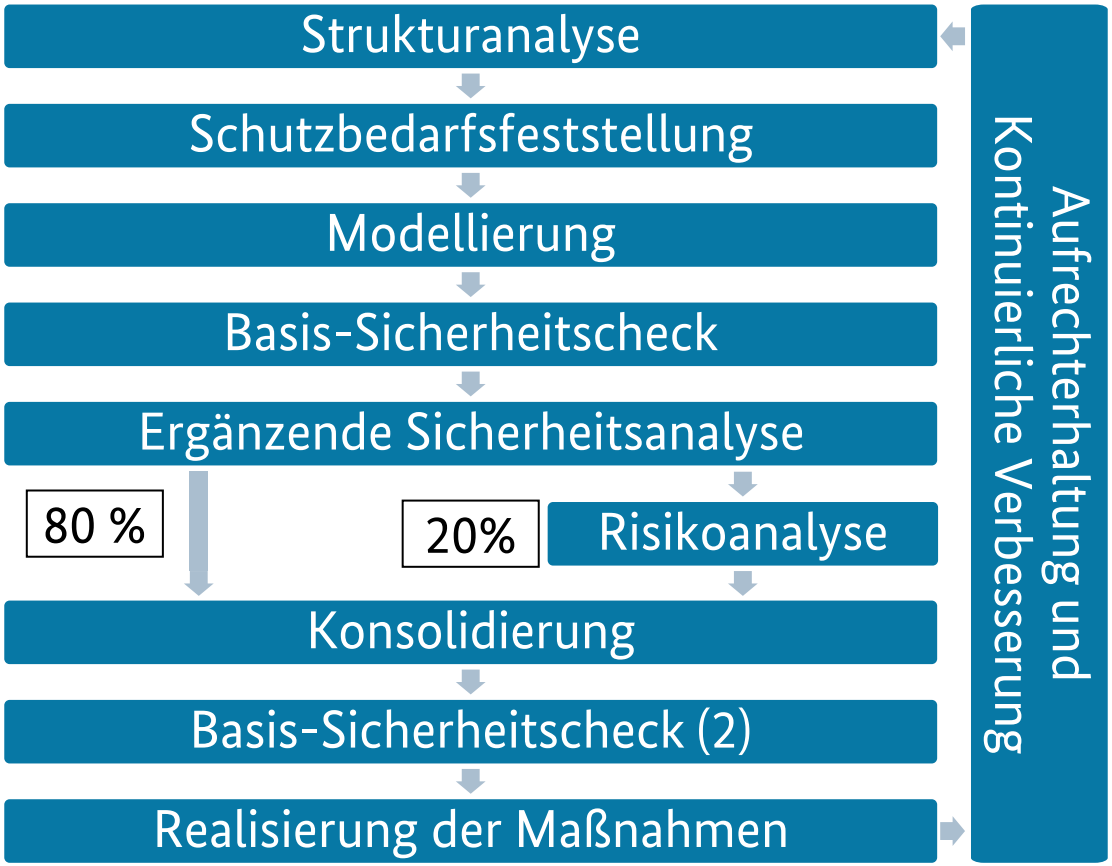
ISO 27005:2011
Status Überarbeitung

- Liaision mit ISO/TC 262, ISO-Committee für ISO 31000 (auch auf Ebene der nationalen Spiegelgremien)
- Integration des Information Security Risk Management in ein integriertes Management System
- Proposal for Title "Information Security Risk Assessment"
- Information Security identifiziert und bewertet Risiken
- Das Risikomanagement der IS-Risiken ist Aufgabe des übergeordneten und organisationsweiten Risk Management Prozesses (Entscheidung, wie mit den Risiken umzugehen ist)

Risikoanalyse nach IT-Grundschutz

Vorarbeiten
Erstellung der Gefährdungsübersicht
Ermittlung zusätzlicher Gefährdungen
Gefährdungsbewertung
Behandlung von Risiken
Konsolidierung

Sicherheitskonzeption nach IT-Grundschutz



BSI Standard 100-3
Risikoanalyse

IT-Grundschutz Teil I

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- Basissicherheitscheck I
- Erg. Sicherheitsanalyse

IT-Grundschutz Teil II

- Basissicherheitscheck II

- Erstellung der Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Gefährdungsbewertung
- Maßnahmenauswahl zur Behandlung von Risiken
- Konsolidierung des Sicherheitskonzepts

Bundesamt für Sicherheit in der Informationstechnik

Erstellung der Gefährdungsübersicht

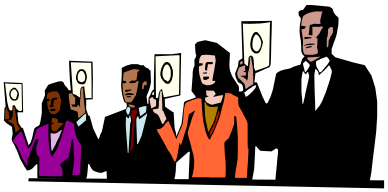
Kommunikationsserver S3	
Vertraulichkeit:	normal
Integrität:	hoch
Verfügbarkeit:	hoch
G 0.8	*Ausfall oder Störung der Stromversorgung*
G 0.9	*Ausfall oder Störung von Kommunikationsnetzen*
G 0.31	*Fehlerhafte Nutzung oder Administration von Geräten und Systemen*
G 0.32	*Missbrauch von Berechtigungen*
G 0.40	*Verhinderung von Diensten (Denial of Service)*
usw.	

Ermittlung zusätzlicher Gefährdungen

- Moderiertes Brainstorming mit klarem Auftrag und Zeitbegrenzung
- Gefährdungen, die nicht in den IT-Grundschutz-Katalogen aufgeführt sind
- Realistische Gefährdungen mit nennenswerten Schäden
- 3 Grundwerte berücksichtigen
- Höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, Außen-/Innentäter
- Externe Quellen einbeziehen

Gefährdungsbewertung

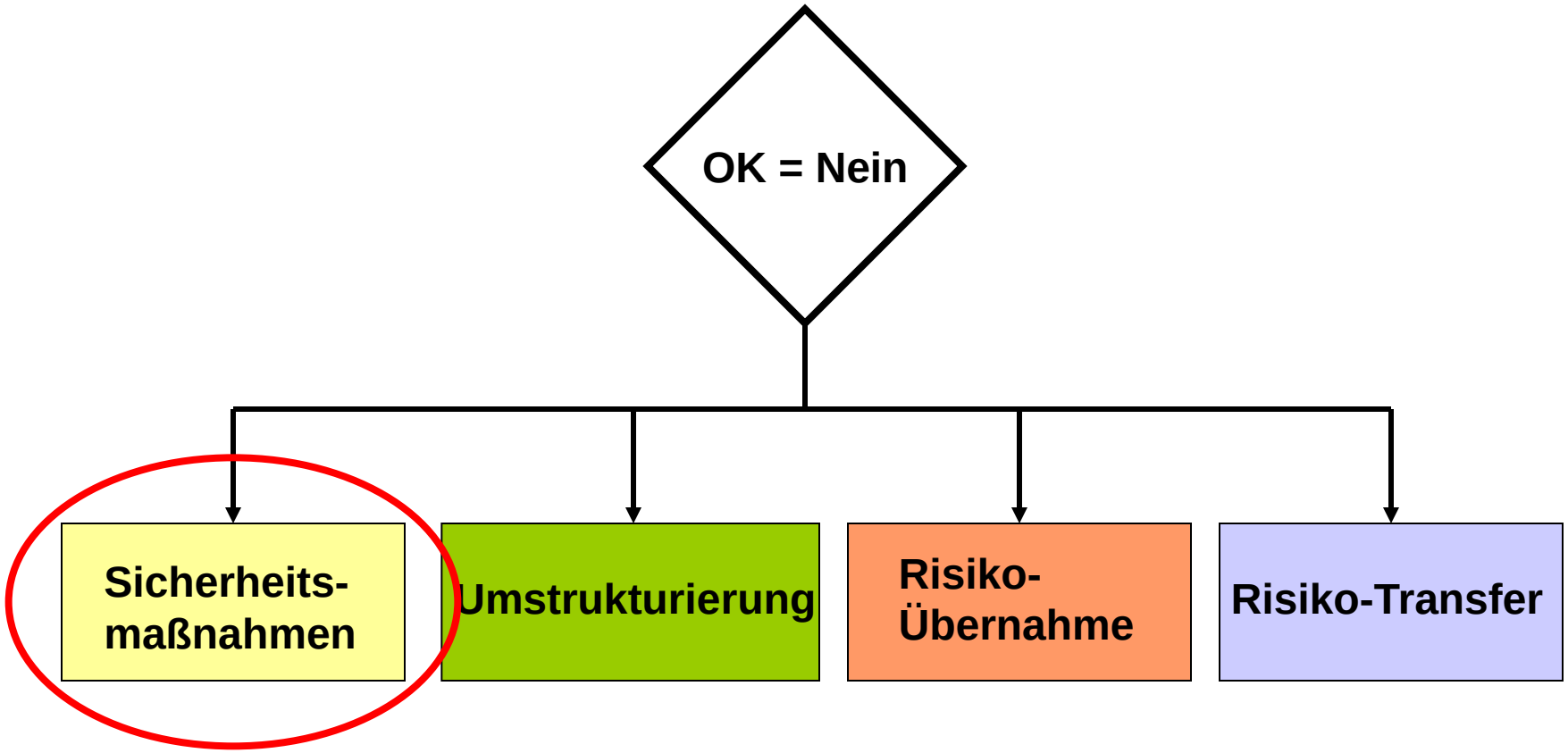
- Sind die vorgesehenen Sicherheitsmaßnahmen ausreichend?
- Prüfung der identifizierten Gefährdungen pro Zielobjekt
- Prüfkriterien:
  - Vollständigkeit
  - Mechanismenstärke
  - Zuverlässigkeit



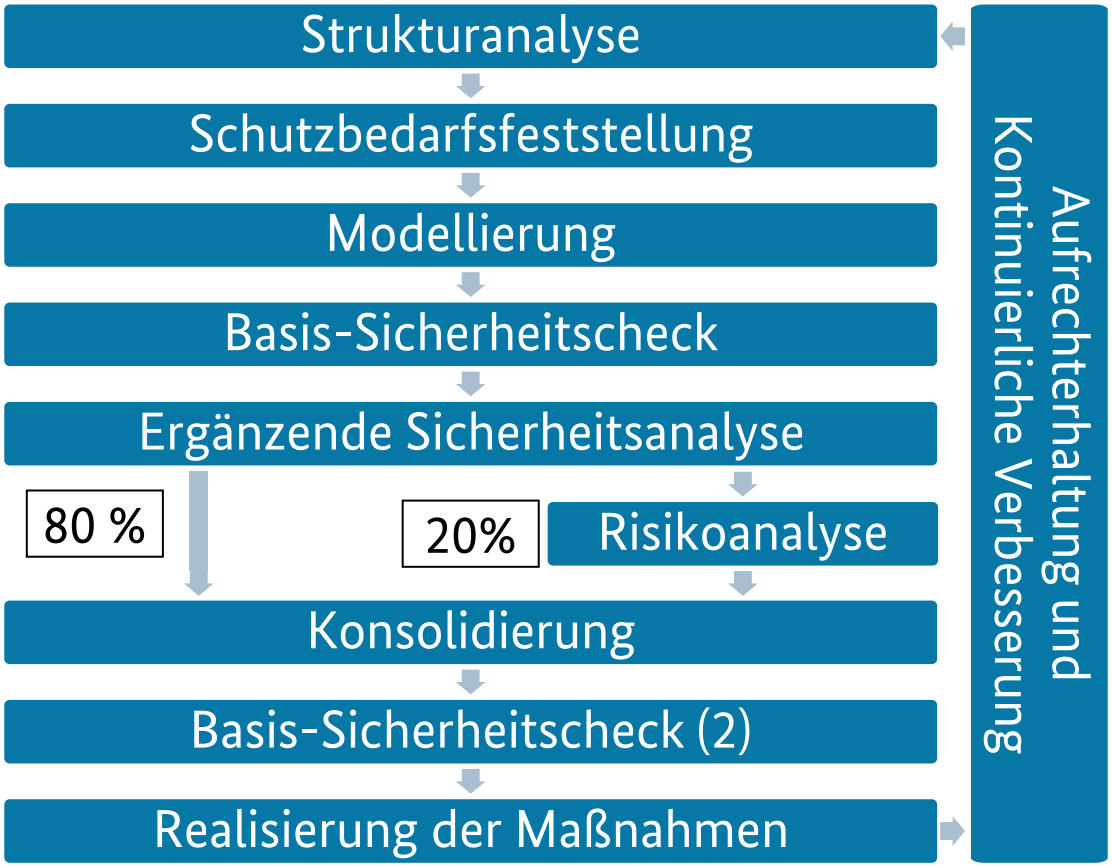
Ergebnis: OK = Ja/Nein

Behandlung von Risiken

Risikobehandlungsoptionen



Sicherheitskonzeption nach IT-Grundschutz



Konsolidierung

- Sind die Sicherheitsmaßnahmen zur Abwehr der jeweiligen Gefährdungen geeignet?
- Wirken die Sicherheitsmaßnahmen sinnvoll zusammen?
- Welche IT-Grundschutzmaßnahmen werden durch höher- oder gleichwertige Maßnahmen ersetzt?
- Sind die Sicherheitsmaßnahmen benutzerfreundlich?
- Sind die Sicherheitsmaßnahmen angemessen?

BSI-Standard 200-X

Zukünftiges Bewertungsverfahren

Neufassung der Risikoanalyse

Bislang:
IT-Grundschutz-spezifisches Verfahren auf der Basis der Gefährdungskataloge

Bündelung aller risikobezogenen Arbeitsschritte in einem neuen BSI-Standard 200-X

Implementation eines Risikoentscheidungsprozesses

Keine Risikoakzeptanz bei den Basis-Anforderungen

Explizite Möglichkeit der Risikoakzeptanz für Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf

Planung BSI-Standard 100-3
Zukünftiges Bewertungsverfahren

Auswirkung / Schaden

Wahrscheinlichkeit	normal	hoch	sehr hoch
sehr wahr-scheinlich			
wahr-scheinlich			
möglich			

Planung BSI-Standard 100-3
Zukünftiges Bewertungsverfahren

Lösungsansätze

- Die Bewertung des Risikos erfolgt durch den populären Matrix-Ansatz anhand weniger Stufen.
- Wenn das Risiko nicht akzeptabel ist, werden Maßnahmen zur Senkung, Vermeidung oder Übertragung des Risikos in Betracht gezogen.
- Im Sinne einer Was-Wäre-Wenn-Analyse wird dann in der Risiko-Matrix "eingezeichnet", wie sich das Risiko bei Umsetzung der jeweiligen Maßnahme ändern würde.
- Dadurch wird automatisch auch das Restrisiko dokumentiert.

Risikoanalyse
-Qualitativ oder quantitiv?

Risikobewertung
Beispiel: Infrastruktur-Risiken
Risikowahrnehmung
Konsolidierung

Qualitativ oder quantitativ?

- ISO 27005:2011: „Risk analysis may be undertaken in varying degrees of detail depending on the criticality of assets, extent of vulnerabilities known, and prior incidents involving in the organization. A risk analysis methodology may be qualitative or quantitative, or a combination of these, depending on the circumstances. In practice, **qualitative analysis is often used first** to obtain a general indication of the level of risk and to reveal the major risks. Later it may be necessary to undertake more specific or quantitative analysis on the major risks because **it is usually less complex and less expensive to perform qualitative than quantitative analysis**."

Qualitativ oder quantitativ?

ISO 31010:
Methods used in analysing risks can be qualitative, semi-quantitative or quantitative.
Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.
Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.
Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.
... it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Qualitativ oder quantitativ?
Überarbeitung ISO 31000

- Goal: to reduce complexity
- Dealing with uncertainty and how to handle it
- Uncertainty can have positive or negative impact: Risks and Opportunities!
- Asset based approach (ISO 55000): assets and their value, value can be tangible/intangible (how to quantify value of intangible assets?)
- Changes: changes either inside or outside the organization may have changed the uncertainties (and thus the basis for assumptions) on which earlier activities and decisions were based.

Risikobewertung

Verbreitet:

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe

Ergebnis: beliebig "genaue" Zahlenwerte

Aber: Wo kommen die Eingangsparameter her?

Schon SiHB: "Für die Ermittlung des Risikos gibt es kein einfaches allgemeingültiges Konzept. ... Im allgemeinen ist die Häufigkeit von seltenen Ereignissen, z. B. von Angriffen auf das IT-System durch Externe, schwer abzuschätzen."

Risikobewertung

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe

Wenig genaue und belastbare Zahlen

Keine allgemein verfügbaren Statistiken

- Erfahrungswerte fehlen
- Dynamisches Umfeld: ständig neue Ideen und Techniken
- Geringe Bereitschaft zur Weitergabe von Schadensereignissen
- Hohe Abhängigkeit von Rahmenbedingungen

Eigene Erhebung lohnt in den wenigsten Fällen

Risikobewertung

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe

Mathematische Herausforderung:

- sehr hoher potentieller Schaden und sehr geringe Eintrittswahrscheinlichkeit
- bereits geringe Fehler bei der Schätzung der Eintrittswahrscheinlichkeit führen zu einer sehr stark verfälschten Einschätzung des Risikos
- Problem der sehr großen und sehr kleinen Zahlen oder $\infty * 1/\infty \neq 1$

Die Mathematik hat Lösungen, z. B. Gauß'sche Fehlerfortpflanzung

Aber: hoher Aufwand!

Beispiel
Infrastruktur-Risiken

Risiko: Blitz

- Beispiel: RZ in München
- DWD-Service: regionales Blitzschlagrisiko
  - Eintrittswahrscheinlichkeit für einen Blitzeinschlag bei 1,24 x 10^{-6} Einschlägen pro Jahr
    (Alle 800.000 Jahre ist mit einem direkten Einschlag zu rechnen)
- Schadenshöhe: mit 10.000 € geschätzt (Neubeschaffung Server)
- Risiko = 1,24 x 10^{-6} x 10.000 € = 0,124
- Vorschlag: äußerer Blitzschutz vorhanden, Installation innerer Blitzschutz (Überspannungsschutz).
- Entscheidung: Risiko tragbar, keine zusätzlichen Maßnahme

Beispiel
Infrastruktur-Risiken

- Leider, leider…
  … halten sich Gewitter nicht an Statistiken
- Blitzeinschlag löste automatische Löschanlage aus
- Stundenlanger RZ-Ausfall, beschädigte Serverkomponenten, umfangreiche Tests und Recovery-Prozeduren, trotzdem Kommunikationsprobleme und unerklärliche Fehler: durch Spannungsspitzen während des Unwetters außerdem Kabel beschädigt
- Gesamtschaden: einige Neubeschaffungskosten, aber hoher Anteil Personalkosten für Fehlersuche, Tests, Wiederanlaufverfahren plus Kosten durch Serverausfälle

Beispiel
Infrastruktur-Risiken

- Leider, leider...
  ... halten sich Gewitter nicht an Statistiken
- Blitzeinschlag löste automatische Löschanlage aus
- Stunde[illegible]enten, umfan[illegible]m Komm[illegible]urch Spannu[illegible]Kabel beschä[illegible]
- Gesamtschaden: einige Neubeschaffungskosten, aber hoher Anteil Personalkosten für Fehlersuche, Tests, Wiederanlaufverfahren plus Kosten durch Serverausfälle

"Zur Wahrscheinlichkeit gehört auch, dass das Unwahrscheinliche eintritt" - Aristoteles

Hypothesen über die Zukunft sind schwierig

...vor allem, wenn wenig Zahlenmaterial über die Vergangenheit vorliegt

Woher nehmen?

- KES
- BKA, FBI und ähnliche Institutionen
- Hersteller und Dienstleister im Umfeld Informationssicherheit
- BSI

Wie zuverlässig?

- Wer wurde gefragt?
- Wer hat ausgewertet? Für welchen Zweck?

Zahlenmaterial

- Gut für Prognosen über Risiko-Trends
- Brauchbare Aussagen über "bewährte" IT-Systeme
- Aber: Risikobewertung für neue Techniken?

Risikowahrnehmung

- Einschätzung von Risiken ist hochgradig subjektiv
- Unterschiedliche Gewinn-, Verlust- und Risikopräferenzen
- Erfolgserwartung: Wo Nutzen erwartet wird, werden höhere Risiken in Kauf genommen.
- Faktor Zeit: Zeitlich weit weg liegende Risiken werden eher akzeptiert als direkt drohende (Rauchen)
- Kontrollmöglichkeit: Dort, wo Personen meinen, das Risiko selber kontrollieren zu können, wird dieses typischerweise unterschätzt (Autounfall versus Flugzeugabsturz).
- Erfahrungswerte: Bekannte Risiken "ungefährlicher" als neue (z. B. Cloud Computing).
- Anzahl Betroffener: Wenn 20 Millionen Menschen für 10 Minuten nicht telefonieren können, wird dies als stärkeres Risiko wahrgenommen, als 2 Tote im Straßenverkehr.

Qualitative vs. quantitative Risikoanalyse

- Erfahrung BSI: Kategorien praktikabler
- Nicht zu wenig, nicht zu viel: drei bis fünf
- Eintrittswahrscheinlichkeit: selten, mittel, häufig, sehr häufig
- Potentielle Schadenshöhe: niedrig, mittel, hoch, sehr hoch
- Genaue, leicht verständliche Beschreibung der Kategorien ist wichtig (Kriterien zur Einordnung)!

Konsolidierung

- **Bei allen Risikobewertungen Ziel nicht vergessen!**
- Angemessene und ausreichende Maßnahmen auswählen
- Sind die Sicherheitsmaßnahmen zur Abwehr der jeweiligen Gefährdungen geeignet?
- Wirken die Sicherheitsmaßnahmen sinnvoll zusammen?
- Sind die Sicherheitsmaßnahmen benutzerfreundlich?
- Sind die Sicherheitsmaßnahmen angemessen?

Fazit

- Quantitative Risikoanalyse aufwändig, langwierig und fehlerträchtig
- Qualitative Risikoanalyse gröber, aber schneller und einfacher (auch verständlicher) - und kann damit auch schneller auf Änderungen reagieren, dahin geht der Trend international (siehe ISO)
- BSI empfiehlt qualitativ
- Besser: Fokus auf Identifikation und Einschätzung von Gefährdungen statt komplexe Risikoberechnungen

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

grundschutz@bsi.bund.de
Tel. +49 (0)22899-9582-5369
Fax +49 (0)22899-10-9582-5369

Bundesamt für Sicherheit in der Informationstechnik
IT-Grundschutz und Allianz für Cyber-Sicherheit
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik