Wirtschaftlichkeitsberechnung von IT-Sicherheitsmaßnahmen

Christian Marx

Vortrag im Seminar IT-Sicherheit am 17. Januar 2018

Lehrstuhl für Wirtschaftsinformatik (Universität Potsdam)

Agenda

1. Motivation
2. Grundlagen
3. Verfahren
4. Zusammenfassung
5. Diskussion

Warum investieren Unternehmen in IT-Sicherheit?

Gesetzliche Vorschriften

Abwenden von Schäden

Effizienzsteigerung von Prozessen

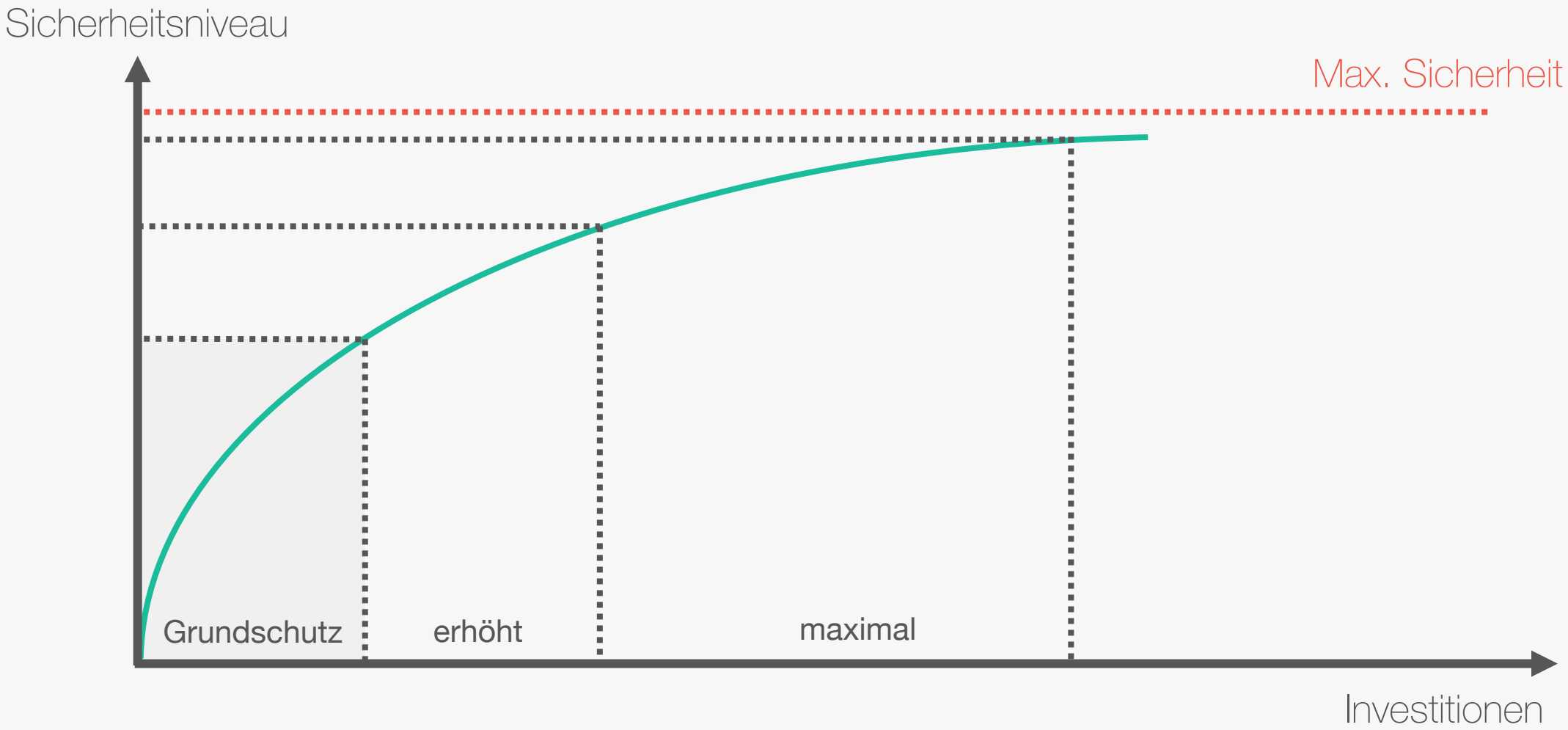
Neue Wertschöpfungspotenziale

Bildquellen: www.pixabay.com (lizenzfreie Bilder)

Der Begriff « Wirtschaftlichkeit »

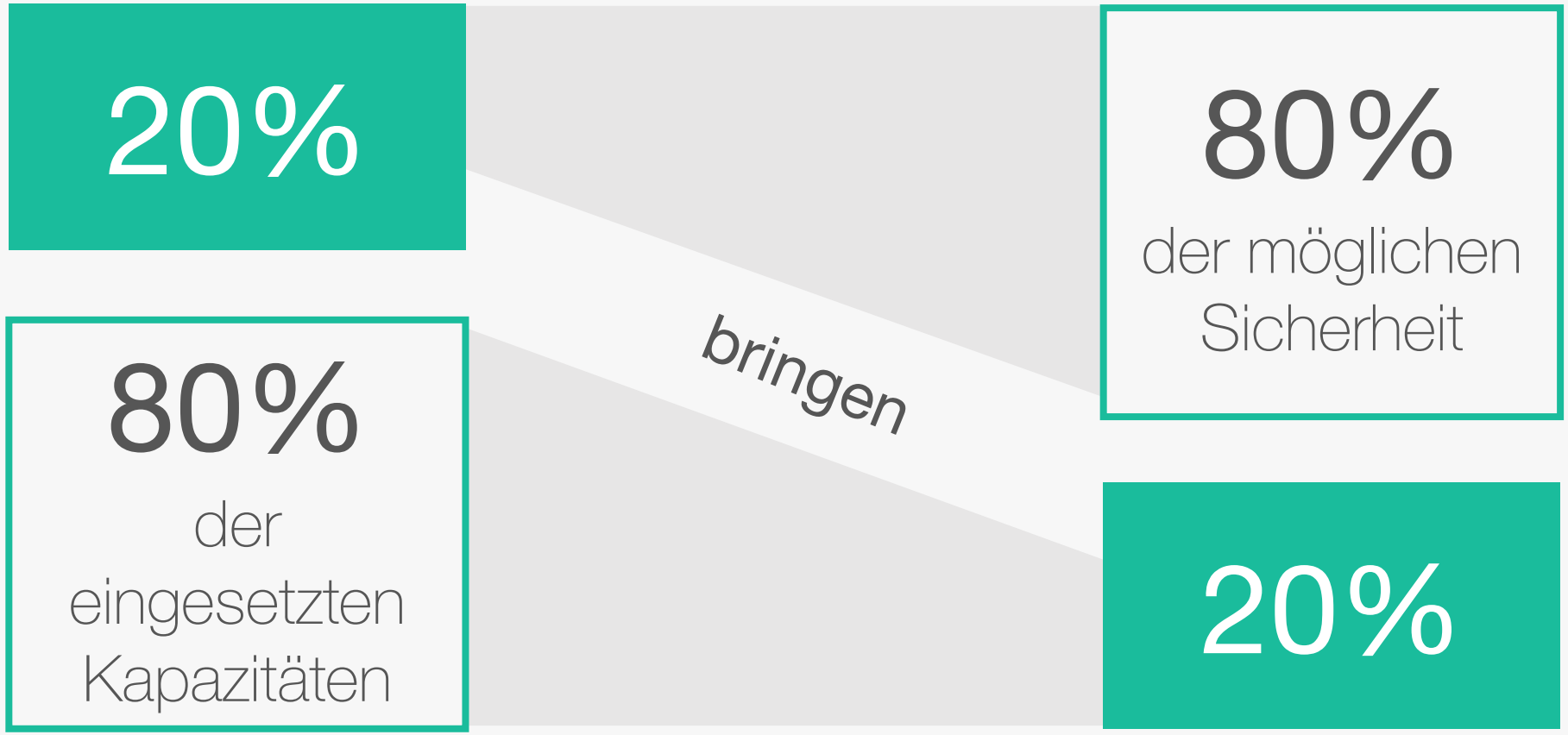
- Verhältnis zwischen **Ergebnis** und **Aufwand**
- Man unterscheidet:
  - **Maximalprinzip** = Bei einem vorgegebenen Aufwand das Ergebnis maximieren.
  - **Minimalprinzip** = Bei einem vorgegebenen Ergebnis den Aufwand minimieren.

Wie viel kostet IT-Sicherheit?



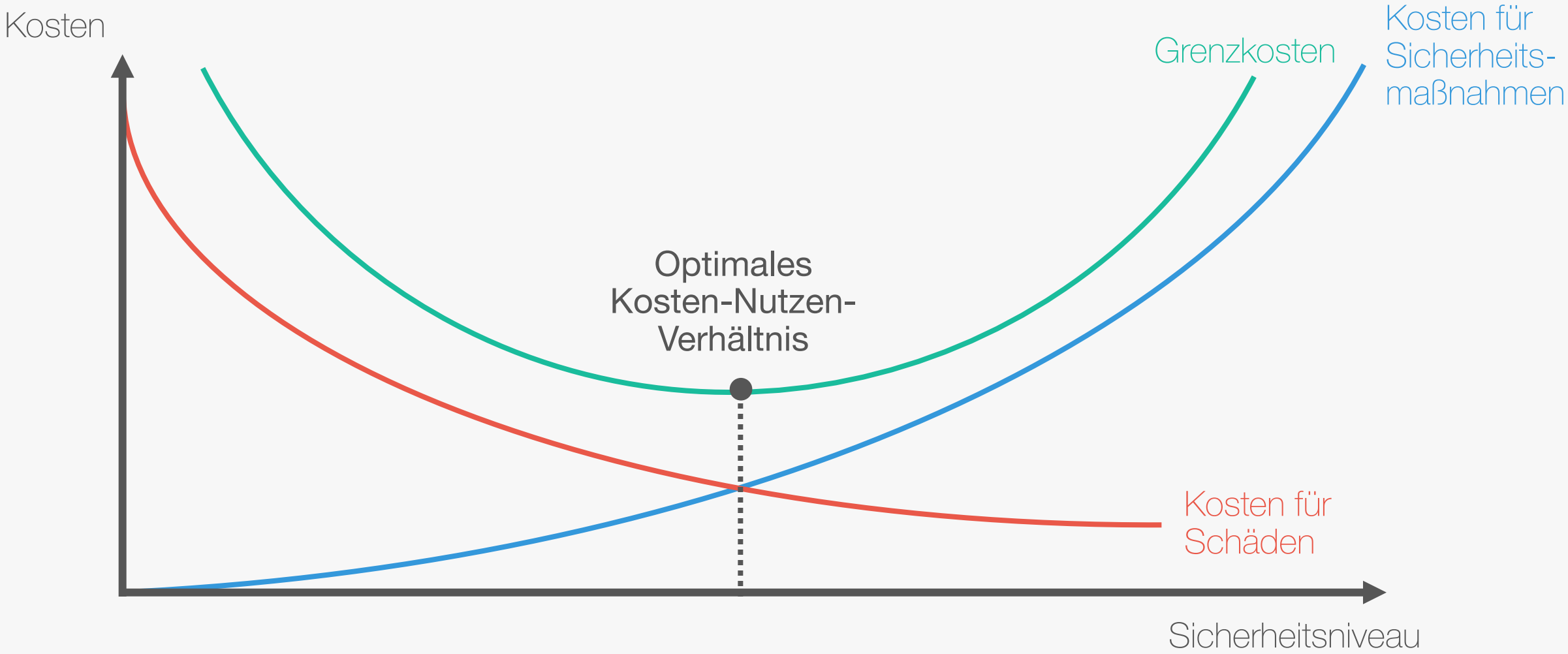
Bildquelle: BSI 100-2

Das Pareto-Prinzip in der IT-Sicherheit



Bildquelle: Eigene Darstellung

Optimales Kosten-Nutzen-Verhältnis



Bildquelle: Hoppe, Prieß & Herne (2003)

Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

TCO
-
Total Costs of Ownership

RoSI
-
Return On Security Investment

WiBe
-
Wirtschaft-lichkeits-betrachtung

QUANTSEC
-
Quantifying Security

Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

TCO
-
Total Costs of Ownership

RoSI
-
Return On Security Investment

WiBe
-
Wirtschaft-lichkeits-betrachtung

QUANTSEC
-
Quantifying Security

Total Costs of Ownership (TCO)

- Klassische **Kostenrechnung**
- **Betrachtung von:**
  - Beschaffungskosten
  - Installationskosten

  } = **Investitionskosten**

  - **Betriebskosten** (z.B. Wartung, Problembehebung, etc.)

Bildquelle: www.pixabay.com (lizenzfreies Bild)

Case-Study: Firewall

Ausgangssituation

- Ein Unternehmen mit 1.000 Mitarbeitern möchte ein professionelles Firewall-System anschaffen.
- Das bevorzugte System kostet in der Anschaffung 40.000 €.
- Die Personalkosten für einen IT-Mitarbeiter betragen 750 € pro Tag.

In Anlehnung an Pohlmann (2015)

Investitionskosten

		Pauschal	Aufwand	Gesamt
Beschaffungs-kosten	Erstellung eines Sicherheitskonzepts	-	25 Tage	18.750 €
	Auswahl des Produkts	-	20 Tage	15.000 €
	Produktkosten	40.000 €	-	40.000 €
Installations-kosten	Installation des Systems	-	10 Tage	7.500 €
	Inbetriebnahme	-	5 Tage	3.750 €
Sonstige Kosten		5.000 €	10 Tage	12.500 €
Gesamtkosten		-	-	92.500 €

Betriebskosten

Beispiel Rechteverwaltung:

- Rechteanpassung je Mitarbeiter: 15 min
- Monatliche Mitarbeiterveränderung: 5%
- 50 Mitarbeiter x 15 min = 750 min → 12,5 h / Monat
- 12,5 h / 8 h * 750 € = **1.171,88 €**

Weitere Betriebskosten für eine Firewall:
Einrichtung neuer Dienste, Updates und Wartung, etc.

Bewertung TCO

Vorteile

- Einfache Rechnung
- Kostentransparenz
- Vergleichbarkeit (z.B. Alternativprodukte, Versicherung, Budget-vorgabe, etc.)

Nachteile

- Keine Berücksichtigung möglicher Risiken
- Nutzung statischer Größen

Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

TCO
-
Total Costs of Ownership

RoSI
-
Return On Security Investment

WiBe
-
Wirtschaft-lichkeits-betrachtung

QUANTSEC
-
Quantifying Security

Return on Security Investment (RoSI)

- ROI = Gegenüberstellung von Kosten und Erlösen
- Bei IT-Security-Investitionen (RoSI) werden klassische Erlöse oft durch monetarisierte Risikobewertungen ersetzt.

Wie können Sicherheitsrisiken sinnvoll bewertet werden?

Risiko =

Schadenshöhe

- Berechnung
- Recherche
- Schätzung

X

Eintritts-wahrscheinlichkeit

- Erfahrungswerte
- Statistiken

Bildquelle: www.pixabay.com (lizenzfreies Bild)

Case-Study: Gestohlene Notebooks

Ausgangssituation

- Nach dem vermehrten Diebstahl von Firmen-Laptops im Außendienst überlegt ein Unternehmen, für alle Geräte eine Festplattenverschlüsselungssoftware einzukaufen.

- **Annahmen:**
  - Benötigte Lizenzen: 300
  - Kosten je Lizenz: 200 € (einmalig)
  - Jährliche Betriebskosten: 10.000 € (im 1. Jahr 15.000 €)

- **Ist eine Investition sinnvoll?**

In Anlehnung an Pohlmann (2015)

Risikoanalyse

- **Frage 1:** Wie viel sind die verlorenen Daten wert bzw. wie hoch ist der jeweils entstandene Schaden?

Schadenshöhe

- **Frage 2:** Mit welcher Wahrscheinlichkeit tritt ein Schadensfall ein?

Eintritts-wahrscheinlichkeit

Zu Frage 1: Schadenshöhe

- Genau beziffern kann das Unternehmen den entstandenen Schaden nicht. Da es sich aber um Kundendaten handelt, beziffert die IT-Abteilung in Absprache mit dem Vertrieb und der Rechts-abteilung den Schaden pro gestohlenem Laptop auf **5.000 Euro**.

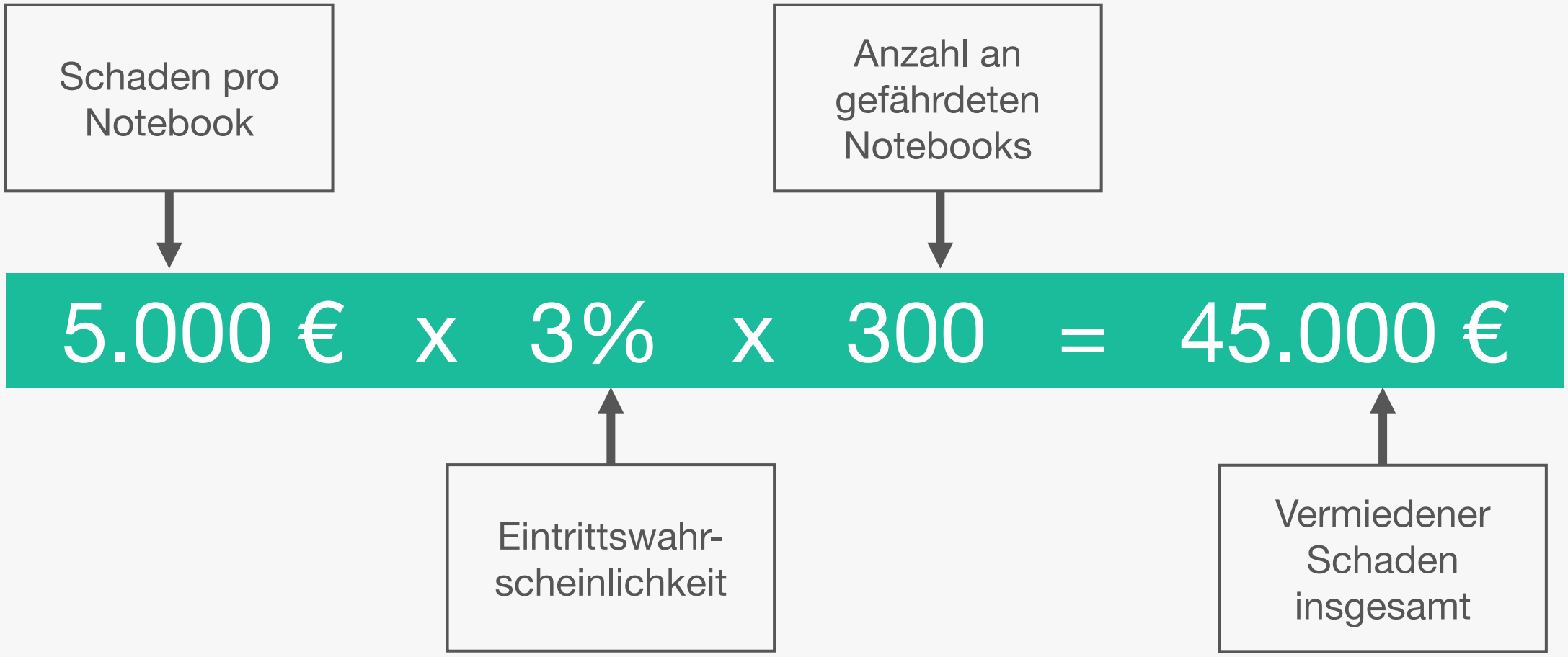
- Der finanzielle Schaden durch Ersatzkäufe für die verlorene Hardware wird hierbei **nicht** berücksichtigt.

Zu Frage 2: Eintrittswahrscheinlichkeit

- Zur Bestimmung der Eintrittswahrscheinlichkeit analysiert das Unternehmen verschiedene Statistiken und gleicht diese mit den eigenen Erfahrungen sowie den Reisezielen der Außendienstmitarbeiter ab.

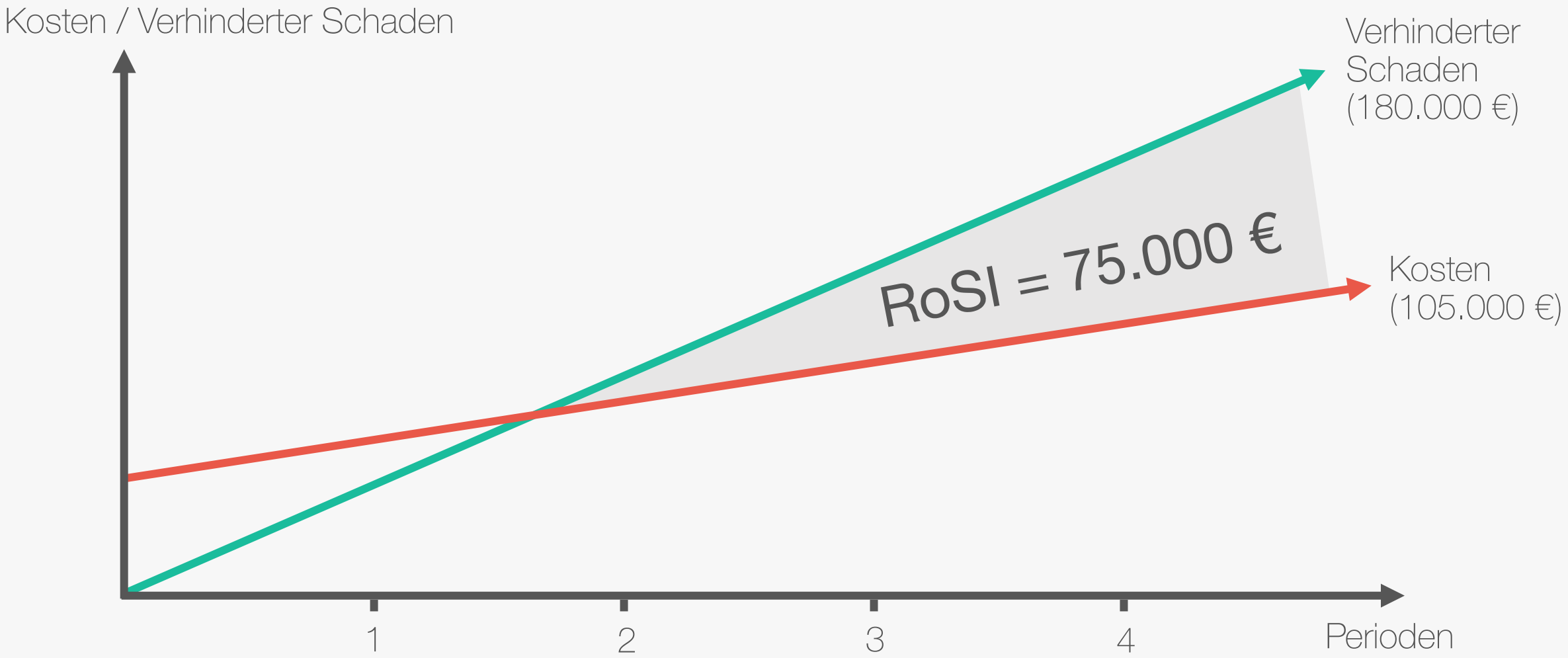
- Insgesamt wird die Eintrittswahrscheinlichkeit auf **3%** festgelegt.

Vermiedener Schaden



	1. Jahr	2. Jahr	3. Jahr	4. Jahr	Summe
Anschaffungs-kosten	60.000 €	-	-	-	60.000 €
Jährliche Betriebskosten	15.000 €	10.000 €	10.000 €	10.000 €	45.000 €
Vermiedener Schaden	45.000 €	45.000 €	45.000 €	45.000 €	180.000 €
RoSI 1. Jahr	- 30.000 €	-	-	-	- 30.000 €
RoSI 2. Jahr	-	35.000 €	-	-	5.000 €
RoSI 3. Jahr	-	-	35.000 €	-	40.000 €
RoSI 4. Jahr	-	-	-	35.000 €	75.000 €

Grafische Darstellung des RoSI



Bildquelle: Eigene Darstellung

Bewertung RoSI

Vorteile

- Einfache Rechnung
- Bewertung von Sicherheitsrisiken
- Bewertung ohne Vergleichsoptionen möglich

Nachteile

- Nutzung statischer Größen
- Bewertung der Sicherheitsrisiken oft schwierig

Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

TCO
-
Total Costs of Ownership

RoSI
-
Return On Security Investment

WiBe
-
Wirtschaft-lichkeits-betrachtung

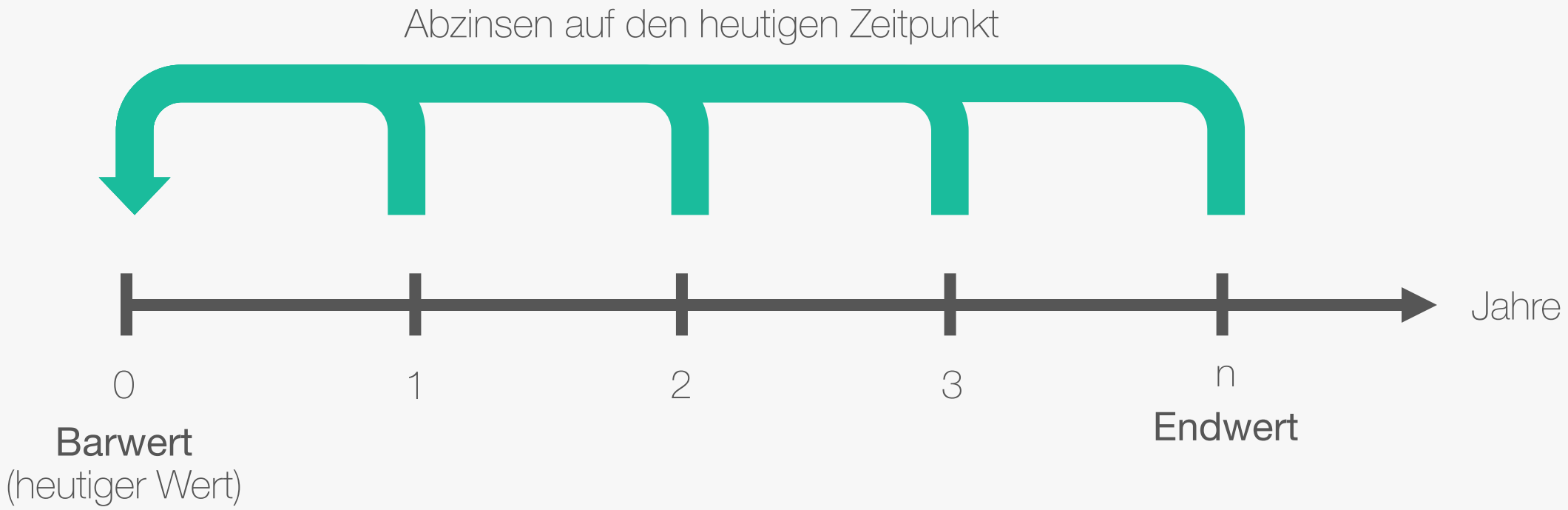
QUANTSEC
-
Quantifying Security

WiBe

- Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der **Bundesverwaltung**, insbesondere beim Einsatz der IT
- Aktueller Stand: **WiBe 5.0** (2014)
- Kein spezieller Fokus auf IT-Sicherheit
- Kombination aus Kapitalwertrechnung und Nutzwertanalyse

Exkurs:
Kapitalwertrechnung und Nutzwertanalyse

Exkurs: Kapitalwertrechnung



Bildquelle: Eigene Darstellung

Exkurs: Kapitalwertrechnung

$$KW_0 = \sum_{t=0}^{n} (E_t - A_t) * d$$

mit

KW_0	Kapitalwert im Bezugszeitpunkt 0
E_t	Einzahlungen am Ende der Periode t
A_t	Auszahlungen am Ende der Periode t
d	Abzinsungsfaktor t Periode (t = 0, 1, 2, 3, ..., n)
n	Betrachtungszeitraum

$$d = \frac{1}{(1+p)^n}$$

mit

d	Abzinsungsfaktor
p	Kalkulationszinsfuß
n	Anzahl Jahre zwischen Zahlung und Basisjahr

Exkurs: Nutzwertanalyse

- Qualitative, nicht-monetäre Analysemethode
- **Nutzen** = Gewichtete Attributausprägungen einer oder verschiedener Handlungsalternativen
- Beispiel:

Auswahl-kriterien	Gewichtung	Alternative 1		Alternative 2	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Kriterium A	70 %	80	56	70	49
Kriterium B	30 %	70	21	50	15
Summe	100 %		**77**		**64**

Bildquelle: www.pixabay.com (lizenzfreies Bild)

Case-Study: Gestohlene Notebooks mit WiBe

Ausgangssituation

- Nach dem vermehrten Diebstahl von Firmen-Laptops im Außendienst überlegt ein Unternehmen, für alle Geräte eine Festplattenverschlüsselungssoftware einzukaufen.

- **Annahmen:**
  - Benötigte Lizenzen: 300
  - Kosten je Lizenz: 200 € (einmalig)
  - Jährliche Betriebskosten: 10.000 € (im 1. Jahr 15.000 €)

- **Ist eine Investition sinnvoll?**

Zusätzliche Angaben

- Kalkulationszinsfuß = 3%
- Beispielrechnung:

$$Abgezinster\ CF\ Jahr\ 1 = \frac{30.000\ €}{(1 + 0{,}03)^1} = 29.126{,}21\ €$$

	Cashflows	Abzinsung	Summe
I_0	- 60.000 €	$-60.000\ €$	- 60.000 €
1. Jahr	30.000 €	$\frac{30.000\ €}{(1+0{,}03)^1} = 29.126{,}21\ €$	- 30.873,79 €
2. Jahr	35.000 €	$\frac{35.000\ €}{(1+0{,}03)^2} = 32.990{,}86\ €$	2.117,07 €
3. Jahr	35.000 €	$\frac{35.000\ €}{(1+0{,}03)^3} = 32.029{,}96\ €$	34.147,03 €
4. Jahr	35.000 €	$\frac{35.000\ €}{(1+0{,}03)^4} = 31.097{,}05\ €$	65.244,08 €

WiBe Q und WiBe E

Nr.	Kriterium	Gewicht	Punkte	Summe
3.1.1	Bedeutung für die IT-Strategie der Behörde	10	6	60
3.1.2	Nachnutzung bereits vorhandener Technologien	10	5	50
3.1.3	Plattform-/Herstellerunabhängigkeit	10	6	60
3.2.1	Qualitätsverbesserung bei der Aufgabenabwicklung	15	6	90
3.2.2	Verkürzung der Durchlaufzeit	15	4	60
3.2.3	Einheitliches Verwaltungshandeln	5	6	30
3.2.4	Imageverbesserung	5	4	20
3.3.1	Informationsbereitstellung und Unterstützung der Entscheidungsträger	15	6	90
3.4.1	Attraktivität der Arbeitsbedingungen	10	8	80
3.4.2	Qualifikationssicherung/-erweiterung	5	4	20
	Summe	100		560
	Qualitätswert			**56**

WiBe Q: Qualitativ-strategische Bedeutung *(Beispiel)*

Nr.	Kriterium	Gewicht	Punkte	Summe
4.1.1	Dringlichkeit aus Nachfrageintensität	10	6	60
4.2.1	Realisierung eines einheitlichen Zugangs	10	5	50
4.2.2	Erhöhung der Verständlichkeit und Transparenz	5	2	10
4.2.3	Hilfefunktionen zur Unterstützung des externen Kunden	5	5	25
4.2.4	Nutzen durch die zeitnahe und vollständige Verfügbarkeit der Information	10	6	60
4.3.1	Wirtschaftlicher Nutzen für den Kunden	25	4	100
4.4.1	Folgewirkungen für den Kommunikationspartner	10	4	40
4.4.2	Auswirkung der Beschleunigung von Verwaltungsentscheidungen für Externe	10	6	60
4.4.3	Verbesserung/Erweiterung des Dienstleistungsangebotes	5	6	30
4.5.1	Nachnutzung von Projektergebnissen	10	6	60
	Summe	100		495
	Externwert			**49**

WiBe E: externe Effekte *(Beispiel)*

Bildquelle: WiBe 5.0

Auswertung der WiBe

WiBe KW > 0 (Kapitalwert = positiv)

+

WiBe Q und / oder WiBe E > 50

Bewertung WiBe

Vorteile

- Klares Vorgehen
- Zukunftsgerichtet
- Monetäre **und** qualitative Faktoren

Nachteile

- Starres „Korsett“
- Fokus auf Behörden
- Höherer Aufwand

4 Genereller Kriterienkatalog für IT-Maßnahmen

Der generelle Katalog enthält alle Kriterien, die in der Regel an eine WiBe angelegt werden können. Neue Kriterienkataloge oder Änderungen an bestehenden Katalogen werden in Kapitel 7 beschrieben.

Wirtschaftlichkeit - Teil Kapitalwertbetrachtung

Alle aus der IT-Maßnahme resultierenden **monetär quantifizierbaren Kosten**- und **Nutzengrößen** sind hier zu erfassen.

Kosten und Nutzen können einmalig und laufend anfallen. Nutzenkriterien können als Einsparungen oder als Mehrerlöse auftreten.

1	**Entwicklungskosten und Entwicklungsnutzen**
1.1	**Entwicklungskosten für die neue IT-Maßnahme**
1.1.1	**Planungskosten**
1.1.1.1	Personalkosten (eigenes Personal)
1.1.1.2	Kosten externer Beratung
1.1.1.3	Kosten der Entwicklungsumgebung
1.1.1.4	Sonstige Kosten für Sach-/Hilfsmittel
1.1.1.5	Reisekosten (eigenes Personal)
1.1.2	**Entwicklungs- und Investitionskosten**
1.1.2.1	Hardwarekosten
1.1.2.1.1	Host/Server, Netzbetrieb
1.1.2.1.2	Arbeitsplatzrechner

1.1.2.2	Softwarekosten
1.1.2.2.1	Kosten für die Entwicklung bzw. Beschaffung von Software
1.1.2.2.2	Kosten für die Anpassung von Software und/oder Schnittstellen
1.1.2.2.3	Kosten für die Evaluierung, Zertifizierung und Qualitätssicherung von Software
1.1.2.3	Installationskosten
1.1.2.3.1	Bauseitige Kosten
1.1.2.3.2	Verlegung technischer Infrastruktur
1.1.2.3.3	Büro-/Raumausstattung, Zubehör
1.1.2.3.4	Personalkosten der Systeminstallation
1.1.3	**Kosten der Systemeinführung**
1.1.3.1	System- und Integrationstest(s)
1.1.3.2	Übernahme von Datenbeständen
1.1.3.3	Erstschulung Anwender und IT-Fachpersonal
1.1.3.4	Einarbeitungskosten Anwender und IT-Fachpersonal
1.1.3.5	Sonstige Umstellungskosten
1.2	**Entwicklungsnutzen aus Ablösung des alten Verfahrens**
1.2.1	**Einmalige Kosteneinsparungen** (Vermeidung von Erhaltungs-/Erweiterungskosten Altsystem)
1.2.2	**Einmalige Erlöse** (aus Verwertung Altsystem)

2	**Betriebskosten und Betriebsnutzen**
2.1	**Laufende Sachkosten/Sachkosteneinsparungen**
2.1.1	**Leitungs-/Kommunikationskosten**
2.1.1.1	Lfd. Kosten aus IT-Maßnahme NEU

Bildquelle: WiBe 5.0

2	Betriebskosten und Betriebsnutzen
2.1.1.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.2	**Host- und Serverkosten**
2.1.2.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.2.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.3	**Kosten für Arbeitsplatzrechner**
2.1.3.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.3.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.4	**Softwarekosten**
2.1.4.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.4.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.5	**Verbrauchsmaterial**
2.1.5.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.5.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.6	**Energie-, Raum- und Klimatisierungskosten**
2.1.6.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.6.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.7	**Kosten externer Unterstützung**
2.1.7.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.7.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.1.8	**Sonstige Kosten**
2.1.8.1	Lfd. Kosten aus IT-Maßnahme NEU
2.1.8.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.2	**Laufende Personalkosten/Personalkosteneinsparungen**
2.2.1	**Personalkosten aus Systembenutzung**
2.2.1.1	Lfd. Kosten aus IT-Maßnahme NEU

2	Betriebskosten und Betriebsnutzen
2.2.1.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.2.2	**Systembetreuung und -administration**
2.2.2.1	Lfd. Kosten aus IT-Maßnahme NEU
2.2.2.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT
2.2.3	**Laufende Schulung/Fortbildung**
2.2.3.1	Lfd. Kosten aus IT-Maßnahme NEU
2.2.3.2	Lfd. Nutzen aus Wegfall IT-Maßnahme ALT

Wirtschaftlichkeit - Teil Nutzwertbetrachtung

Qualitativ-strategische Bedeutung der IT-Maßnahme

Diese Kriterien bewerten das Neusystem und lassen sich nur qualitativ beschreiben.

3	Qualitativ-strategische Kriterien
3.1	**Bedeutung der IT-Maßnahme**
3.1.1	**Bedeutung für die IT-Strategie der Behörde**
3.1.2	**Nachnutzung bereits vorhandener Technologien**
3.1.3	**Plattform-/Herstellerunabhängigkeit**
3.2	**Qualitätszuwachs bei der Erledigung von Fachaufgaben**
3.2.1	**Qualitätsverbesserung bei der Aufgabenabwicklung**
3.2.2	**Verkürzung der Durchlaufzeit**
3.2.3	**Einheitliches Verwaltungshandeln**
3.2.4	**Imageverbesserung**
3.3	**Informationen für die Entscheidungsträger**
3.3.1	**Informationsbereitstellung und Unterstützung der Entscheidungsträger**

Bildquelle: WiBe 5.0

3.4	**Mitarbeiterbezogene Effekte**
3.4.1	**Attraktivität der Arbeitsbedingungen**
3.4.2	**Qualifikationssicherung/-erweiterung**

Externe Effekte der IT-Maßnahme

IT-Maßnahmen, die Auswirkungen auf Kunden (Bürger, Unternehmen, andere Verwaltungseinheiten) haben, werden mit diesen Kriterien qualitativ erfasst.

4	**Externe Effekte**
4.1	**Ablösedringlichkeit aus Perspektive des externen Kunden**
4.1.1	**Dringlichkeit aus Nachfrage(-intensität)**
4.2	**Benutzerfreundlichkeit aus Kundensicht**
4.2.1	**Realisierung eines einheitlichen Zugangs**
4.2.2	**Erhöhung von Verständlichkeit und Transparenz**
4.2.3	**Hilfefunktion zur Unterstützung des externen Kunden**
4.2.4	**Nutzen durch die zeitnahe und vollständige Verfügbarkeit der Information**
4.3	**Wirtschaftliche Effekte extern**
4.3.1	**Wirtschaftlicher Nutzen für den Kunden**
4.4	**Qualitäts- und Leistungssteigerungen**
4.4.1	**Folgewirkungen für den Kommunikationspartner**
4.4.2	**Auswirkung der Beschleunigung von Verwaltungsentscheidungen für Externe**
4.4.3	**Verbesserung / Erweiterung des Dienstleistungsangebotes**
4.5	**Synergien**
4.5.1	**Nachnutzung von Projektergebnissen**

Der generelle Kriterienkatalog dient als Checkliste:

Im ersten Schritt Ihrer WiBe ziehen Sie den generellen Kriterienkatalog heran, um die für Ihre Maßnahmen relevanten Kriterien zu bestimmen. Beachten Sie, dass der Kriterienkatalog Vollständigkeit anstrebt.

- Wählen Sie aus dem generellen Kriterienkatalog nur die für Ihre Maßnahme relevanten Kriterien aus.
- Daneben kann es für Sie relevante Kriterien geben, die nicht auf den ersten Blick im generellen Kriterienkatalog verzeichnet sind. In diesem Falle gehen Sie wie folgt vor:
  a) Prüfen Sie, ob Ihr Kriterium sich unter einem Kriterium des generellen Kriterienkatalogs subsumieren lässt (siehe Kapitel 5 – ausführliche Beschreibung der Einzelkriterien). In diesem Fall ist bei dem Kriterium ggf. eine Erläuterung erforderlich.
  b) Lässt sich Ihr Kriterium nicht unter ein Kriterium des generellen Kriterienkatalogs subsumieren, können Sie ein zusätzliches Kriterium in einem neu zu erstellenden speziellen Kriterienkatalog aufnehmen (siehe Kapitel 7).

Bildquelle: WiBe 5.0

Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen

TCO
-
Total Costs of Ownership

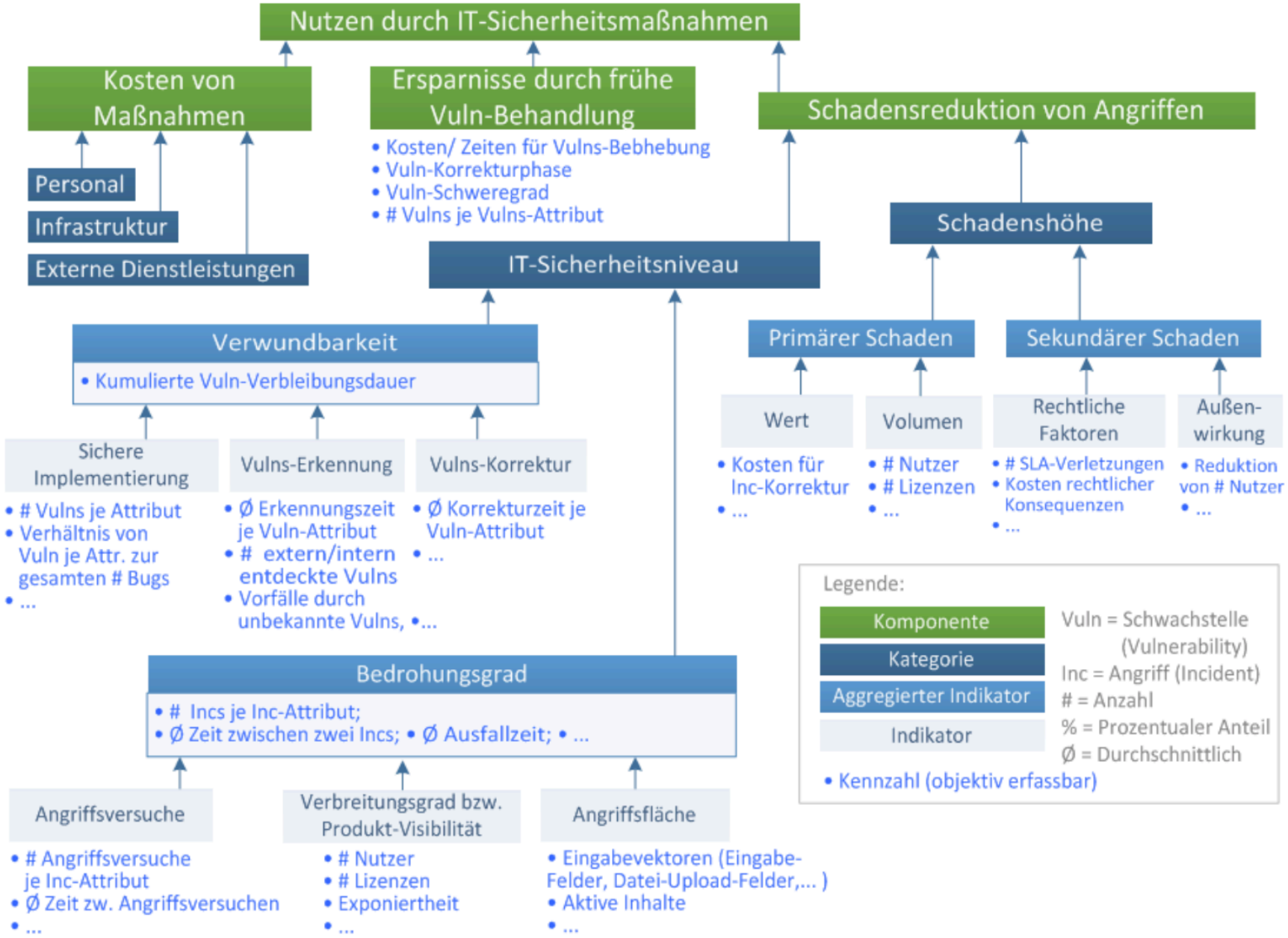
RoSI
-
Return On Security Investment

WiBe
-
Wirtschaft-lichkeits-betrachtung

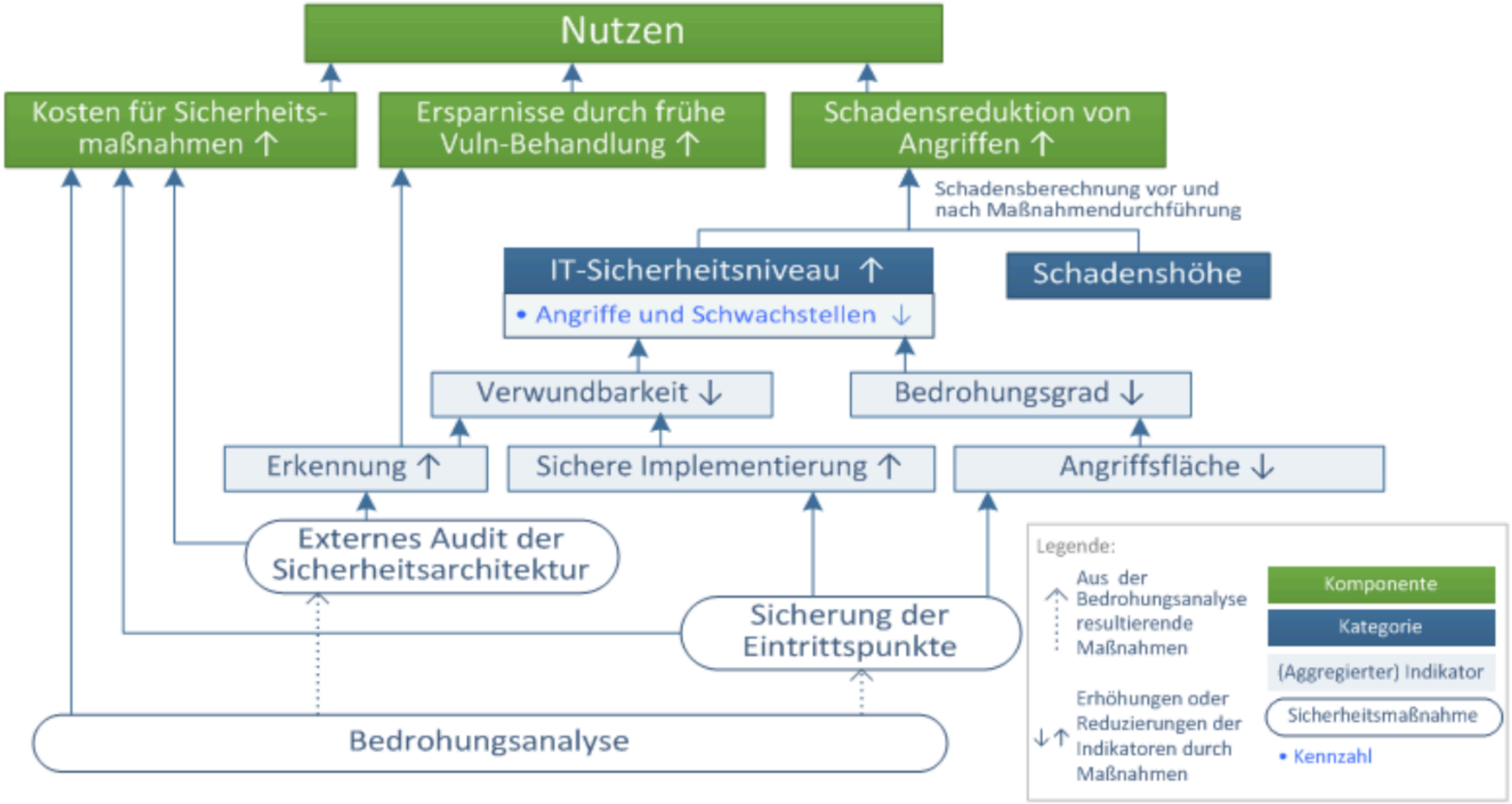
QUANTSEC
-
Quantifying Security

QUANTSEC

- **Quant**ifying **Sec**urity
- **Hierarchisches Vorgehensmodell** zur objektiven, kontinuierlichen und automatisierbaren Messung des Nutzens von IT-Sicherheitsmaßnahmen
- **Nachgelagerte Analyse** von Maßnahmen in fixen Zeitabschnitten (z.B. 6 Monate)
- Fokus auf Software-Entwicklung



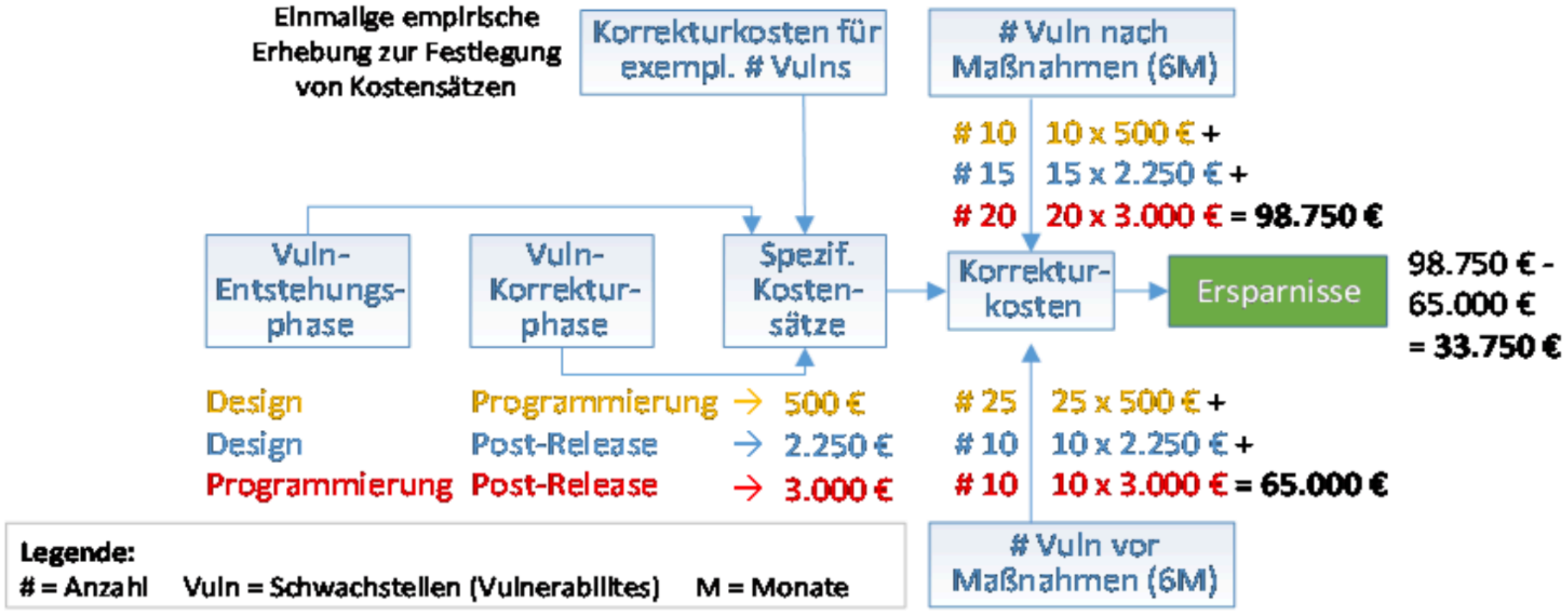
Bildquelle: Chehrazi, Schmitz & Hinz (2015)



Bildquelle: Chehrazi, Schmitz & Hinz (2015)

Case-Study: Software Engineering

Bildquelle: www.pixabay.com (lizenzfreies Bild)



Bildquelle: Chehrazi, Schmitz & Hinz (2015)

Bewertung QUANTSEC

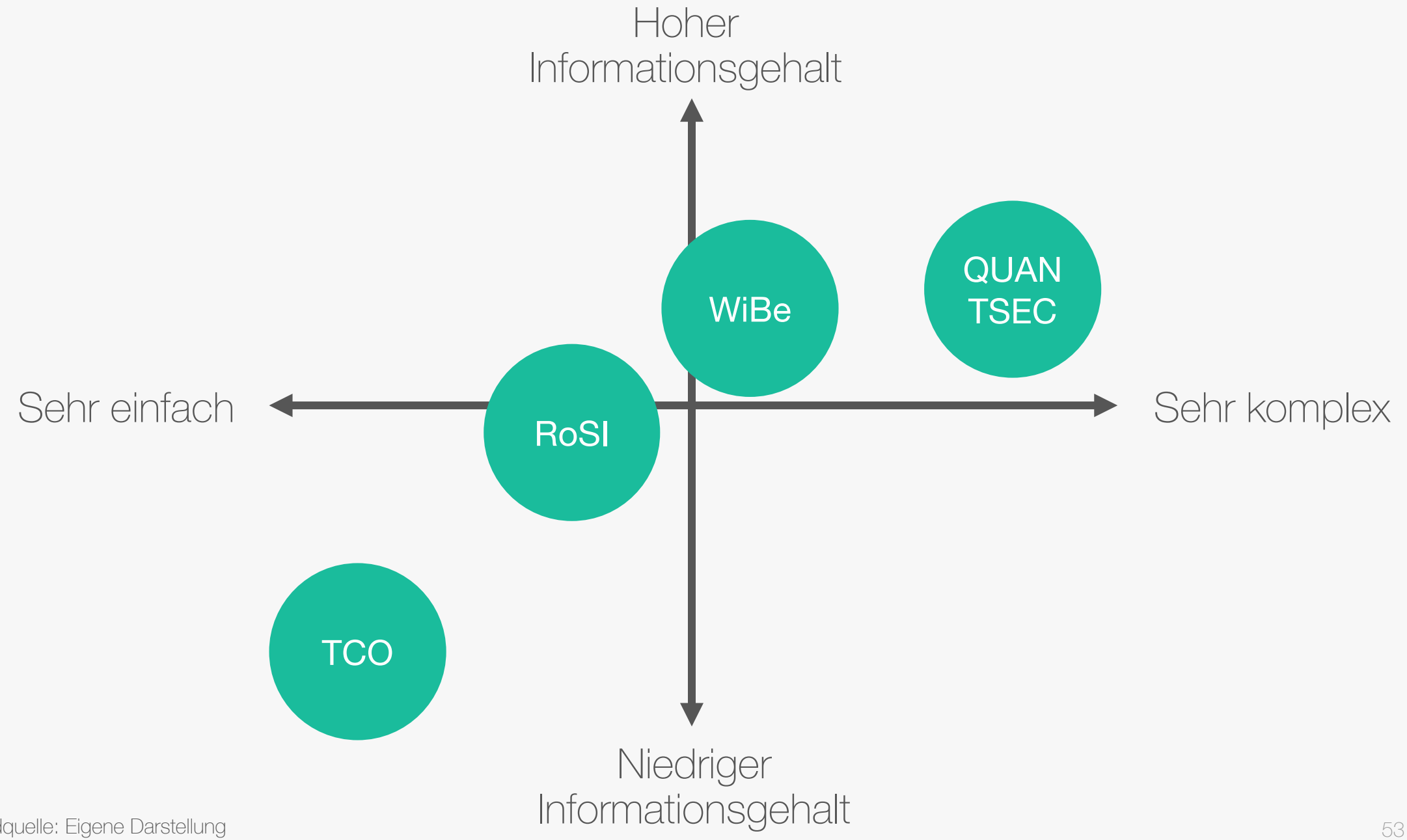
Vorteile

- Hohe Objektivität
- Hohe Transparenz
- Schafft Bewusstsein für Themen

Nachteile

- Komplexität des Verfahrens
- Vergangenheitsorientiert
- Fokus auf Software-Entwicklung

Zusammenfassung und Einordung

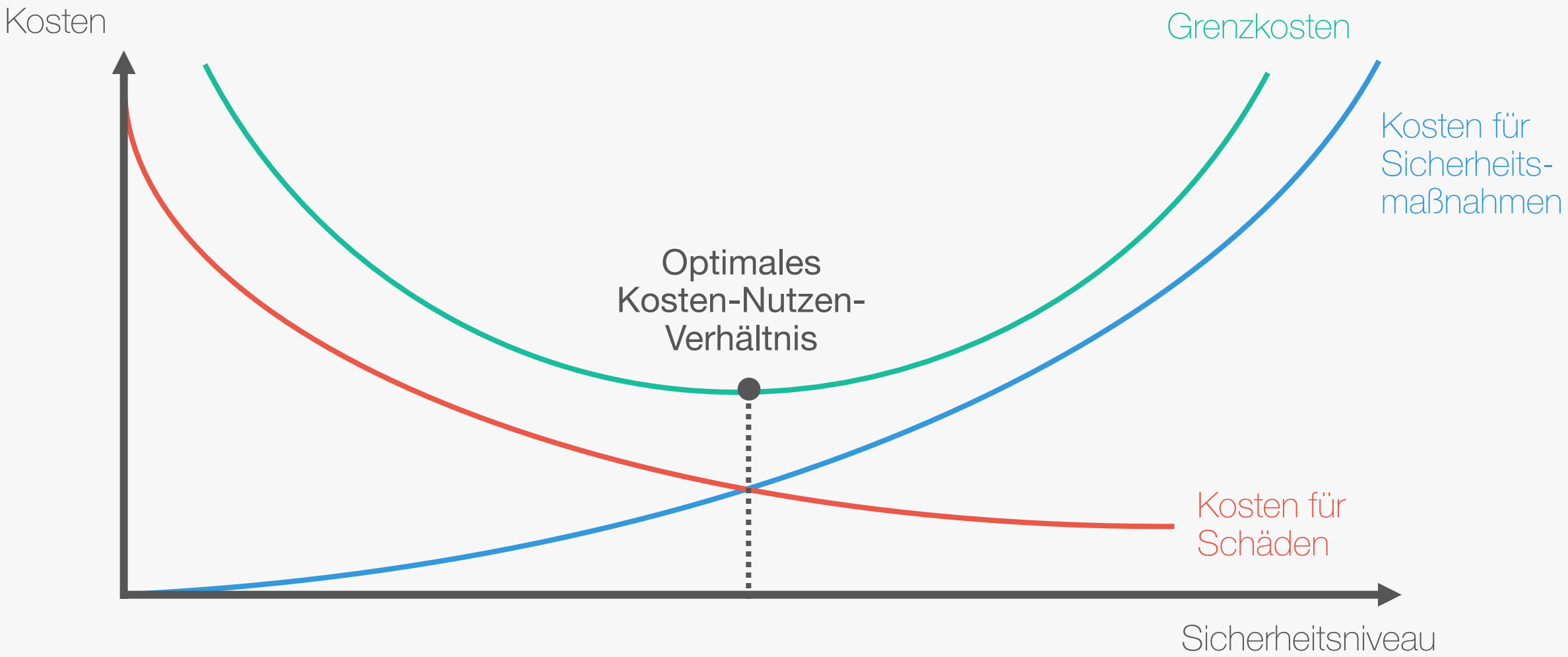


Bildquelle: Eigene Darstellung

Diskussion

- Wann können Investitionen in IT-Sicherheitsmaßnahmen trotz negativem RoSI dennoch sinnvoll sein?

Optimales Kosten-Nutzen-Verhältnis



Bildquelle: Hoppe, Prieß & Herne (2003)

Diskussion

- Wann können Investitionen in IT-Sicherheitsmaßnahmen trotz negativem RoSI dennoch sinnvoll sein?
- **Wie wird sich die Digitalisierung auf die Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen auswirken?**

Diskussion

- Wann können Investitionen in IT-Sicherheitsmaßnahmen trotz negativem RoSI dennoch sinnvoll sein?
- Wie wird sich die Digitalisierung auf die Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen auswirken?
- **Investieren Unternehmen zu viel oder zu wenig in IT-Sicherheitsmaßnahmen?**

“The greatest IT risk facing most companies is more prosaic than a catastrophe. It is, simply, overspending.“

Nicolas G. Carr

Quellenverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2008): **BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise**. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=1, zuletzt geprüft am 14.01.2018.

Bundesamt für Sicherheit in der Informationstechnik (2017): **Die Lage der IT-Sicherheit in Deutschland 2017**. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 14.01.2018.

Carrn Nicholas (2003): IT Doesn‘t Matter. In: Harvard Business Review, Vol. 0305 (2003), S. 5-17.

Chehrazi, Golriz; Schmitz, Christopher & Hinz, Oliver (2015): **QUANTSEC – Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen**. In: Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1131-1145.

Quellenverzeichnis

Die Beauftragte der Bundesregierung für Informationstechnik (2014): **WiBe 5.0 - Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT**. Online verfügbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/WiBe_50.pdf?__blob=publicationFile, zuletzt geprüft am 14.01.2018.

Fraunhofer-Institut für Sichere Informationstechnologie Darmstadt (2011): **Werte schützen, Kosten senken, Erträge steigern**. White Paper, Sankt Augustin.

Hoppe, Gabriela & Priess, Andreas (2003): **Sicherheit von Informationssystemen: Gefahren, Maßnahmen und Management im IT-Bereich**. Herne: NWB, Verlag Neue Wirtschaftsbriefe.

Nowey, Thomas; Federrath, Hannes; Klein, Christian; Plößl, Klaus (2005): **Ansätze zur Evaluierung von Sicherheitsinvestitionen**. In: Sicherheit 2005. Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics (P-62), Köllen Verlag, Bonn 2005, 15-26.

Quellenverzeichnis

Pohlmann, Norbert (2015): **Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen**, Fachhochschule Gelsenkirchen, Fachbereich Informatik. Online verfügbar unter https://norbert-pohlmann.com/app/uploads/2015/08/155-Wirtschaftlichkeitsbetrachtung-von-IT-Sicherheitsmechanismen-Prof.-Norbert-Pohlmann.pdf, zuletzt geprüft am 14.01.2018.

Rumpel, Rainer (2007): **Verfahren zur Wirtschaftlichkeitsanalyse von Investitionen in IT-Sicherheit - Eine Vorstudie**. Fachhochschule für Wirtschaft Berlin, Fachbereich Berufsakademie. Online verfügbar unter http://www.rumpel.de/Forschung/Vorstudie.pdf, zuletzt geprüft am 14.01.2018.

Sonnenreich, Wes; Albanese, Jason & Stout, Bruce (2006): **Return On Security Investment (ROSI) - A Practical Quantitative Model**. In: Journal of Research and Practice in Information Technology 32 (1), S. 45-56.

Soo Hoo, Kevin (2000): **How Much Is Enough? A Risk-Management Approach to Computer Science**. Working Paper, Consortium for Research on Information Security and Policy (CRISP).

Zantow, Roger & Dinauer, Josef (2011): **Finanzwirtschaft des Unternehmens** (3., überarb. Aufl.). München: Pearson Studium.