

# IT-Frühwarnsysteme im Bankenumfeld

Matthias Stoffel

Berlin, 13. Mai 2004

## Agenda

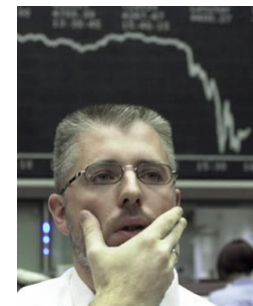
1. Frühwarnung und Prognosen im Bankenumfeld
2. Anforderungen an ein IT-Frühwarnsystem
3. Umgang mit (Früh-) Warnungen in der Sparkassen-Finanzgruppe
4. Randbedingungen für ein IT-Frühwarnsystem

**Ich kann zwar die Bahn der Gestirne  
auf Zentimeter und Sekunden berechnen,  
aber nicht,  
wohin eine verrückte Menge einen  
Börsenkurs treibt.**

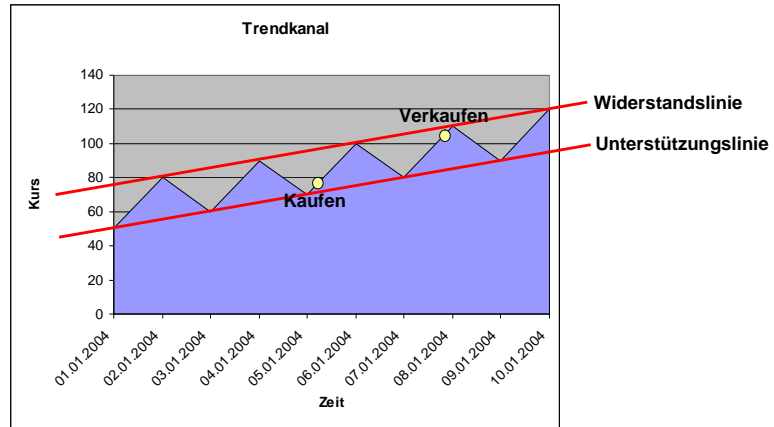
Isaac Newton 1643-1725

## Prognosen für die Börse

- **Research**
  - Politik
  - Allgemeine Marktstimmung
  - Gewinnentwicklung von Unternehmen
  - Fusionen/Übernahmen von Unternehmen
  - In und Out – Branchen
  - Gerüchte
  - ...
- **Messbare Einflussfaktoren**
  - Teuerungsrate
  - Leitzinsen
  - Währungskurse
  - ...
- **Kurse der Vergangenheit**

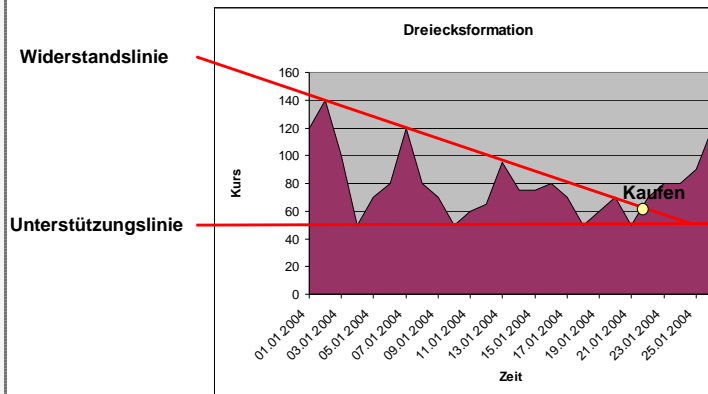


■ Trendanalysen – der Trendkanal



# Kurse der Vergangenheit verlaufen in einem Dreieck?

■ Trendanalysen - die Dreiecksformation



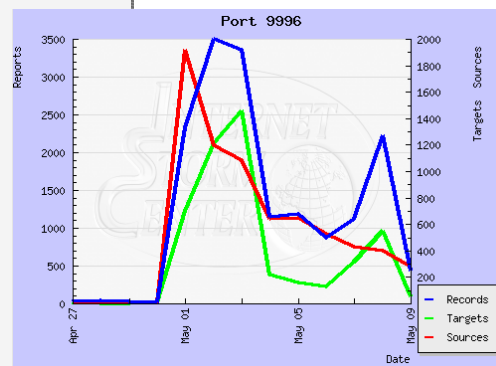
■ Durchschnittslinien



**Suchen und Ersetzen:**

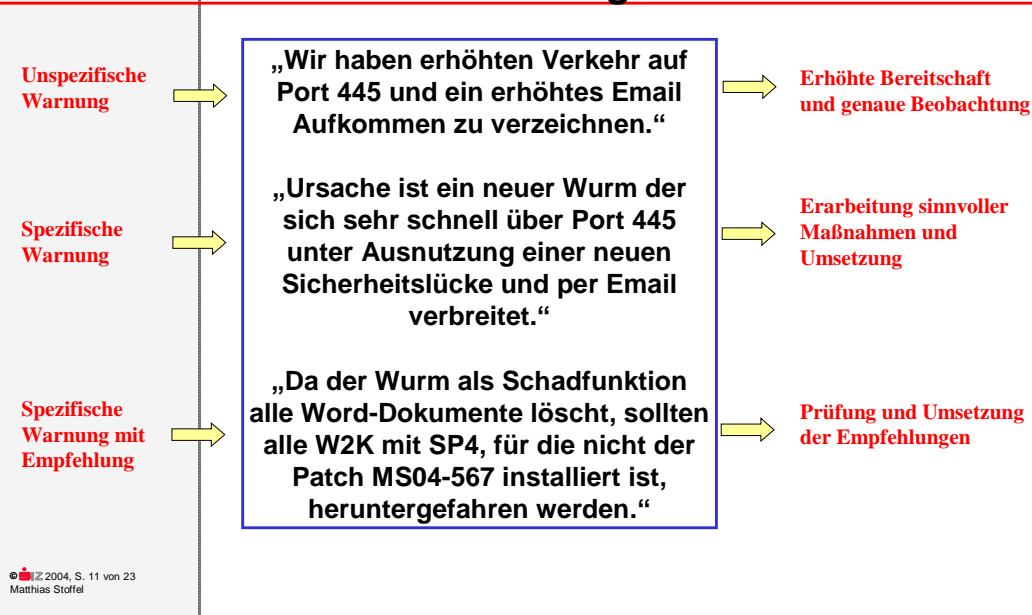
**„Kurs“ durch „Portzugriffe“  
und  
„Verkaufen“ durch „Alarm“.**

1. Frühwarnung und Prognosen im Bankenumfeld
2. Anforderungen an ein IT-Frühwarnsystem
3. Umgang mit (Früh-) Warnungen in der Sparkassen-Finanzgruppe
4. Randbedingungen für ein IT-Frühwarnsystem

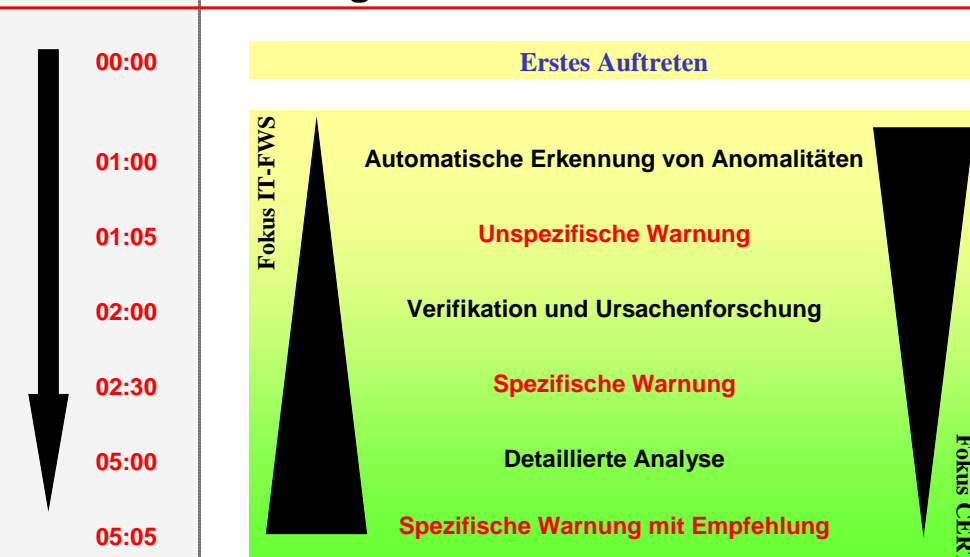


Date	Sources	Targets	Records
2004-05-09	279	56	439
2004-05-08	401	550	2227
2004-05-07	426	314	1124
2004-05-06	523	131	868
2004-05-05	645	161	1189
2004-05-04	640	221	1146
2004-05-03	1086	1458	3359
2004-05-02	1194	1211	3494
2004-05-01	1919	700	2328
2004-04-30	4	5	11
2004-04-29	6	3	22
2004-04-28	9	3	36
2004-04-27	9	4	32

## Wie könnten Warnungen aussehen?



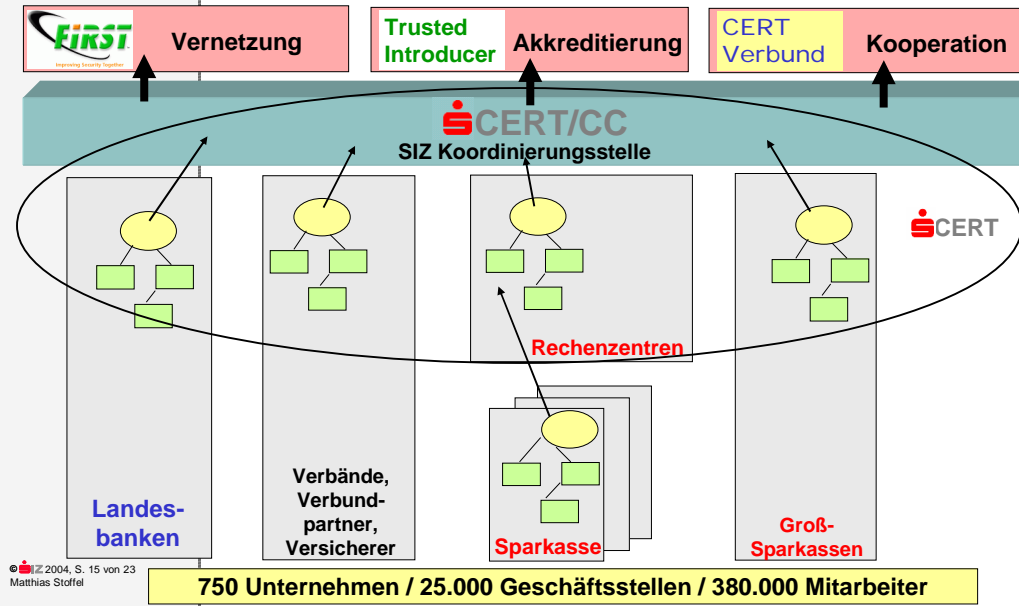
## Wie lange könnte es dauern?



- Email
- Out-of-Band als Fax / Telefon

1. Frühwarnung und Prognosen im Bankenumfeld
2. Anforderungen an ein Frühwarnsystem
3. Umgang mit (Früh-) Warnungen in der Sparkassen-Finanzgruppe
4. Randbedingungen für ein IT-Frühwarnsystem

# Sicherheitsrisiken.

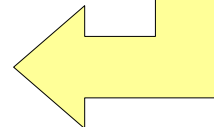


© SIZ 2004, S. 15 von 23  
Matthias Stoffel

# Allen SIZ CERT Warnungen wird ein Risikowert zugeordnet.

		Schadenshöhe				
		GERING	GERING-MITTEL	MITTEL	MITTEL-HOCH	HOCH
Angriffswahrscheinlichkeit	GERING	■■■■	■■■■■	■■■■■	■■■■■	■■■■■
	GERING-MITTEL	■■■■	■■■■■	■■■■■	■■■■■	■■■■■
	MITTEL	■■■■	■■■■■	■■■■■	■■■■■	■■■■■
	MITTEL-HOCH	■■■■	■■■■■	■■■■■	■■■■■	■■■■■
	HOCH	■■■■	■■■■■	■■■■■	■■■■■	■■■■■

Risiko = 3

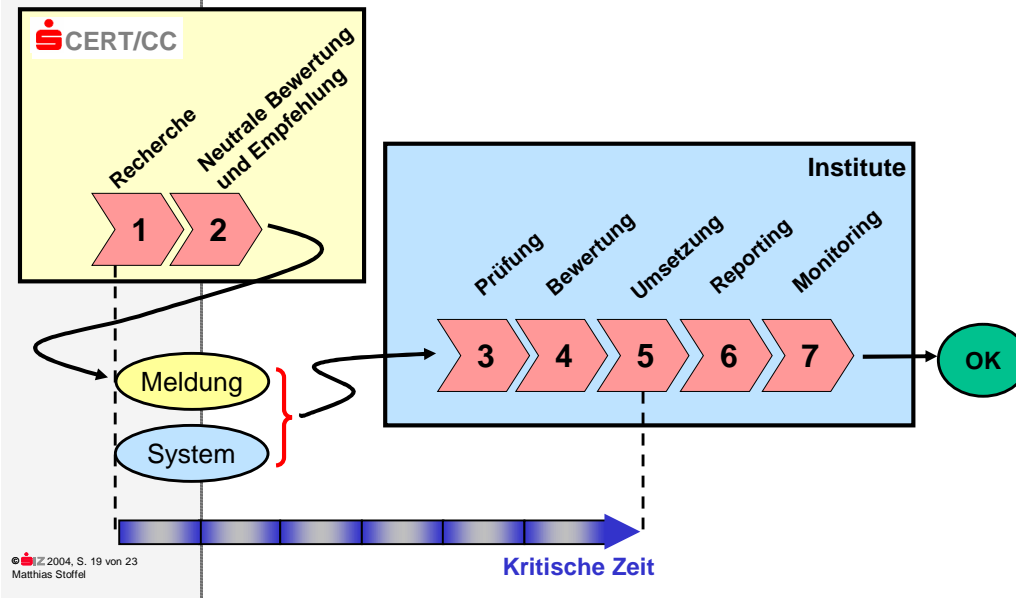


- **Keine Reaktion**
- **Langfristige Reaktion**  
Umsetzung zum nächsten Änderungstermin
- **Mittelfristige Reaktion**  
Umsetzung im nächsten Wartungsfenster
- **Kurzfristige Reaktion**  
Umsetzung während des Betriebes mit Tests
- **Sofortige Reaktion**  
Umsetzung während des Betriebes auch ohne Tests

## In Abhängigkeit vom Risiko wird die Reaktionsgeschwindigkeit festgelegt.

### System x

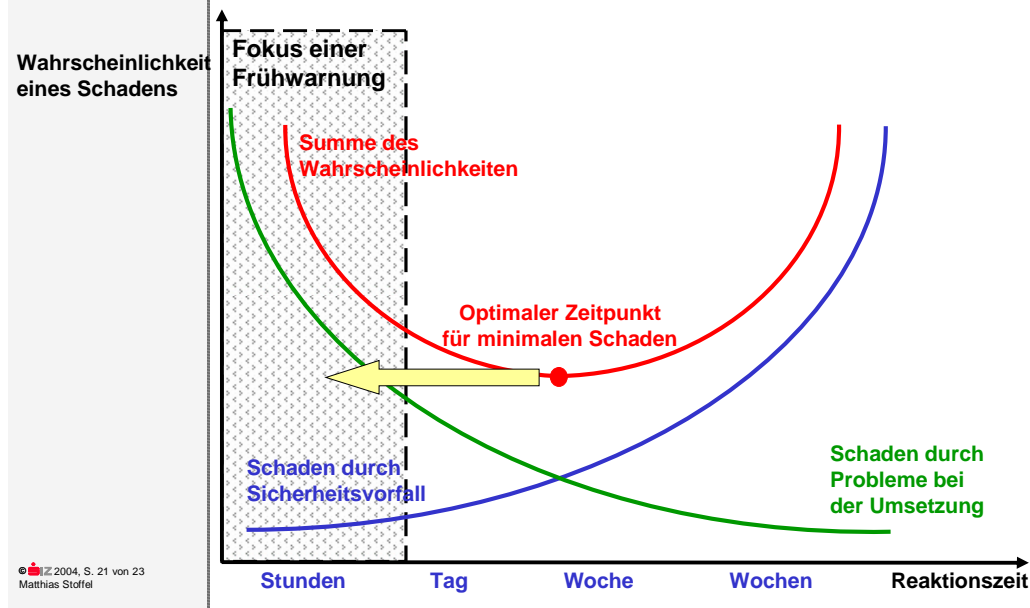
- Risiko 1 → Keine Reaktion
- Risiko 2 → Keine Reaktion
- Risiko 3 → Mittelfristige Reaktion
- Risiko 4 → Mittelfristige Reaktion
- Risiko 5 → Kurzfristige Reaktion



## Agenda

1. Frühwarnung und Prognosen im Bankenumfeld
2. Anforderungen an ein Frühwarnsystem
3. Umgang mit (Früh-) Warnungen in der Sparkassen-Finanzgruppe
4. Randbedingungen für ein IT-Frühwarnsystem

## Beachtung?



## Welche Punkte können den Erfolg eines IT-FWS unterstützen?

- Festlegung der Szenarien für die ein IT-FWS Unterstützung bieten soll – z. B. Warnungen vor:
  - Zielgerichteten Angriffen
  - Sicherheitslücken
  - Malware
  - ...
- Abgrenzung zu Antiviren-Labors, CERTs und IDS.
- Warnungen nur für Gefahren mit entsprechend hoher Angriffswahrscheinlichkeit und hohem potenziellen Schaden.
- Fokus auf Empfehlungen die unmittelbar und ohne große Störungen umgesetzt werden können.

- Etablierte wissenschaftliche Methoden zur automatisierten Auswertung sind wichtig.
- Wünschenswert sind spezifische Warnungen mit Empfehlungen.
- CERT könnten ihre Arbeit auf Basis der Ergebnisse eines IT-FWS stützen.
- Wer ein IT-FWS sinnvoll nutzen möchte, muss Prozesse zum Umgang mit Warnungen etabliert haben.
- Überlegungen für welche Szenarien ein IT-FWS zum Einsatz kommen soll, sind wesentlich.

