IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

Universität Hildesheim
Institut für Betriebswirtschaftslehre und Wirtschaftsinformatik

FINANZ_IT Hannover
OE 2152 „Endgeräte“

IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

1. Einleitung

2. Sicherheitskonzeption

2.1 Ausgangsanalyse

2.2 Schwachstellenanalyse

2.3 Risikobehandlung

3. Zusatzaktivitäten

4. Fazit

IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

1. Einleitung

2. Sicherheitskonzeption

2.1 Ausgangsanalyse

2.2 Schwachstellenanalyse

2.3 Risikobehandlung

3. Zusatzaktivitäten

4. Fazit

- Ausgangssituation
  - Unsichere IT-Welt
  - Bedrohungen nehmen stetig zu
  - Heutige Sicherheitsgewährleistung < 100%
- Folglich
  - Wie erreicht man einen höchstmöglichen Sicherheitsstand?
  - Welche Vorgehensweise ermöglicht die Erfüllung dieses Ziels?

IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

1. Einleitung

2. Sicherheitskonzeption

2.1 Ausgangsanalyse

2.2 Schwachstellenanalyse

2.3 Risikobehandlung

3. Zusatzaktivitäten

4. Fazit

- Sicherheitskonzeption einer Thin Client Plattform
  - Hardware: Server, Clients und Peripherie
  - Software: Management-Tool (Server) und Betriebssystem (Client)
- Herausforderungen
  - Einbettung der Plattform in bestehende Infrastruktur
  - Analyse der Kommunikationswege
  - Schwachstellen erkennen
  - Gegenmaßnahmen erarbeiten

Quelle: Fujitsu Siemens

→ Gewährleistung eines sicheren Produktiveinsatzes

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

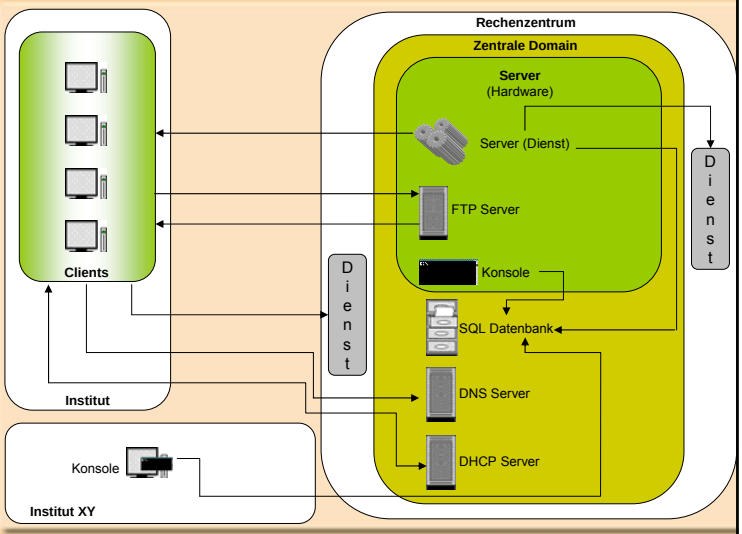
Wann und womit beginnen? (1/2)

- IT-Sicherheit beginnt mit dem Kick-Off eines Projekts
  - Analyse von
    - Bestehender Infrastruktur / Produktionsumgebung
    - Neu-Komponenten
    - Interaktion- und Kommunikation zwischen alter und neuer Welt
- Ziel
  - Erfassung / Betrachtung aller zentralen und peripheren Einflussfaktoren
  - Gesamtüberblick über Soll- und Ist-Zustand

→ Sicherheit ist hier noch kein zentrales Thema

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

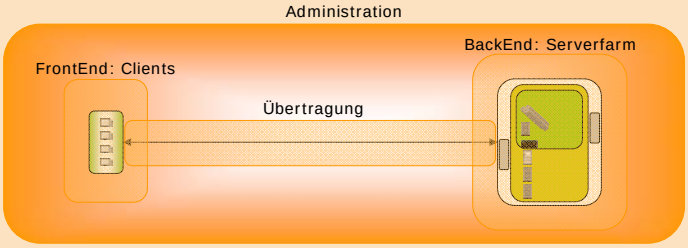
Wann und womit beginnen? (2/2)



1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Erste Schritte zum sicheren System (1/4)

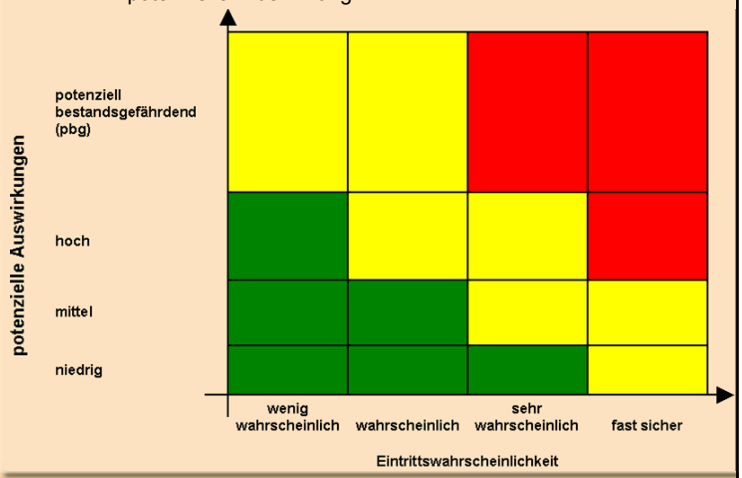
- Ermittlung von Schwachstellen
  - Bestimmung potenzieller Bedrohungen
    - Unterscheidung hinsichtlich des Orts des Auftretens



1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Erste Schritte zum sicheren System (2/4)

- Bewertung bezüglich Eintrittswahrscheinlichkeit und potenzieller Auswirkung



1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Erste Schritte zum sicheren System (3/4)

- Definition von
  - Sicherheitsfunktionen
    - Integrierte Maßnahmen und Eigenschaften der Komponente zum Schutz selbiger und ihrer Daten
  - Sicherheitsannahmen
    - Bereits eingerichtete und etablierte Schutzmechanismen
  - Sicherheitsanforderungen
    - Nicht existierende Schutzmechanismen
- Ergebnis
  - Folgerung von Schwachstellen der Neu-Komponente

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Erste Schritte zum sicheren System (4/4)

- Ergebnismatrix

	SF_1:	SF_2:	SA_1:	SA_2:	SAF_1:	SAF_2:	Ergebnis
B_FrontEnd_1					0		SW_1
B_FrontEnd_2					0		SW_2
...							
B_Ubertragung_1			+				+
...							
B_Admin_1							+
...							
B_BackEnd_1						0	SW_12
B_BackEnd_2				+			+
...							

Legende:
„0“ – Schutzmechanismus wirkt nicht ausreichend gegen Bedrohung
„+“ – Schutzmechanismus wirkt vollständig gegen Bedrohung

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Behandlung entdeckter Schwachstellen (1/2)

- Definition von Gegenmaßnahmen
  - Verbesserung der aktuellen Situation
  - Lang- oder kurzfristige Abwendung der Schwachstellen
  - Arten von Gegenmaßnahmen
    - Definitiver Lösungsweg
    - Möglicher Lösungsansatz
- Ziel
  - Nachträgliche Behebung der Schwachstellen
  - Minimierung von Eintrittswahrscheinlichkeit und / oder Auswirkung

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Behandlung entdeckter Schwachstellen (2/2)

- Ergebnismatrix

Maßnahmen / Schwachstellen	M_1	M_2	M_3	M_4	M_5	Ergebnis
SW_1:	+					Schwachstelle behoben.
SW_2:	+					Schwachstelle behoben.
SW_3:		+				Schwachstelle behoben.
SW_4:		+				Schwachstelle behoben.
SW_5:			0			Restrisiko RR_1
SW_6:			0	0		Restrisiko RR_2
SW_7:						Restrisiko RR_3
SW_8:					+	Schwachstelle behoben.

Legende:
„0“ – Maßnahme wirkt nicht ausreichend gegen Schwachstelle
„+“ – Maßnahme wirkt vollständig gegen Schwachstelle

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

- Prüfung der Restrisiken hinsichtlich deren Eintrittswahrscheinlichkeit und Auswirkung
  - Restrisiko sehr wahrscheinlich und potenziell bestandsgefährdend?
    - Kommunikation mit Zulieferer
    - Worst-case: Projektstop, kein Produktiveinsatz der Komponente
  - Restrisiko unwahrscheinlich und geringe Auswirkung?
    - Dokumentation der Risiken
    - Offenlegung der Risiken
    - Risikoübernahmeerklärung
    - Freigabe des Projekts

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

- Parallele Tests der Komponente
  - Unhabhängige Einheit zur Prüfung der Ergebnisse aus der Entwicklung
  - Einheit zur Prüfung und Abnahme der Sicherheitsvorkehrungen

→ Ergebnisse fließen wiederum in die Entwicklung ein

- Katastrophen-Management
  - Weiterführendes Konzept zur Definition von Vorgehensweisen bei Eintritt einer Beeinträchtigung der Infrastruktur oder einzelner Komponenten

IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

- Umfassende, dokumentierte Analyse der Plattform
  - Einzelkomponenten auf Hard- und Softwareebene
  - Kommunikationsbeziehung zwischen bestehender und zu integrierender Infrastruktur
- Sicherheitstechnisch geprüftes System
  - Definition interner und externer Sicherheitsmechanismen
  - Dokumentation aller akuten Restrisiken
  - Aufnahme in Katastrophen-Konzept
- Zentrale Wissensbasis zur sicheren Implementierung der Plattform

→ Minimierung des Gesamtrisikos des Produktiveinsatzes

IT-Sicherheit im Bankenumfeld: Ein konzeptioneller Ansatz

1. Einleitung
2. Sicherheitskonzeption
2.1 Ausgangsanalyse
2.2 Schwachstellenanalyse
2.3 Risikobehandlung
3. Zusatzaktivitäten
4. Fazit

Danke für ihre Aufmerksamkeit