IT-Incident Management durch externe Dienstleistung - Die Lösung aller IT-Incident Management Probleme ?

Roland Wagner

Roland.Wagner@datev.de

Agenda

- Kurze Vorstellung DATEV
- Sichere Netzwerke
- Datenreduktion
- Managed Security Services
- Anforderungen an MSS
- Zusammenfassung


DATEV

DATEV: Das Unternehmen

DATEV eG

- Hauptsitz: Nürnberg
  Gründung: 1966

Einzige berufsständische EDV-Dienstleistungsorganisation in Europa für

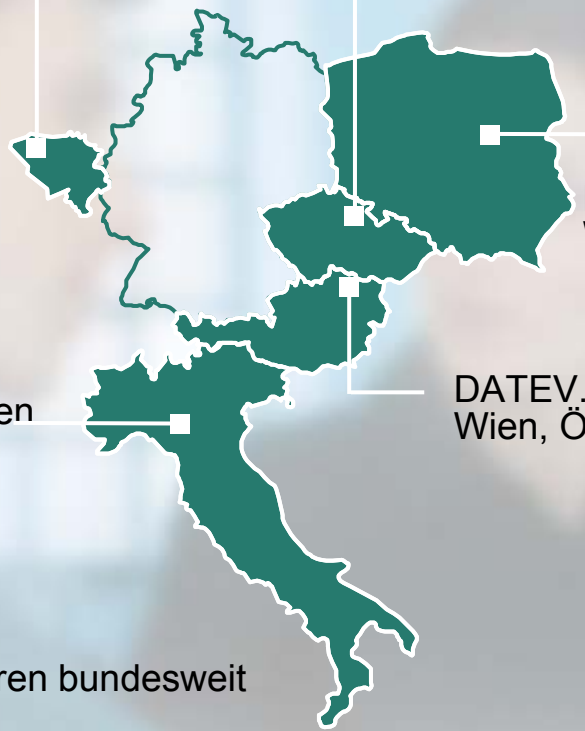
- Steuerberater
- Rechtsanwälte
- vereidigte Buchprüfer
- Wirtschaftsprüfer

DATEV: Das Unternehmen

Informationszentren, Informationsbüro Brüssel und verbundene Unternehmen

Brüssel, Belgien:
Informationsbüro

Verbundene Unternehmen:
DATEV.cz s.r.o.
Brünn, Tschechien



DATEV Symfonia
Warschau, Polen

D&K S.r.l.
Mailand, Italien

DATEV.at GmbH
Wien, Österreich

26 Informationszentren bundesweit

DATEV: Auftrag und Mitglieder

Unser Auftrag

- Wirtschaftliche Förderung unserer Mitglieder (38.943 in 2002)
- Das bedeutet: Unterstützung bei allen Dienstleistungen, unserer Mitglieder für deren Mandanten

Unsere Mitglieder

- Steuerberater
- Rechtsanwälte
- Wirtschaftsprüfer
- vereidigte Buchprüfer
- Steuerberatungs-gesellschaften
- Wirtschaftsprüfungs-gesellschaften
- Buchprüfungsgesellschaften
- Rechtsanwaltsgesellschaften

DATEV: Produktsortiment

Datenverarbeitung

z.B.

- Datentransfer
- Langzeit Archivierung
- Rechenzentrums-verarbeitung

Service

z.B.

- Consulting
- Training
- IT Support

Software

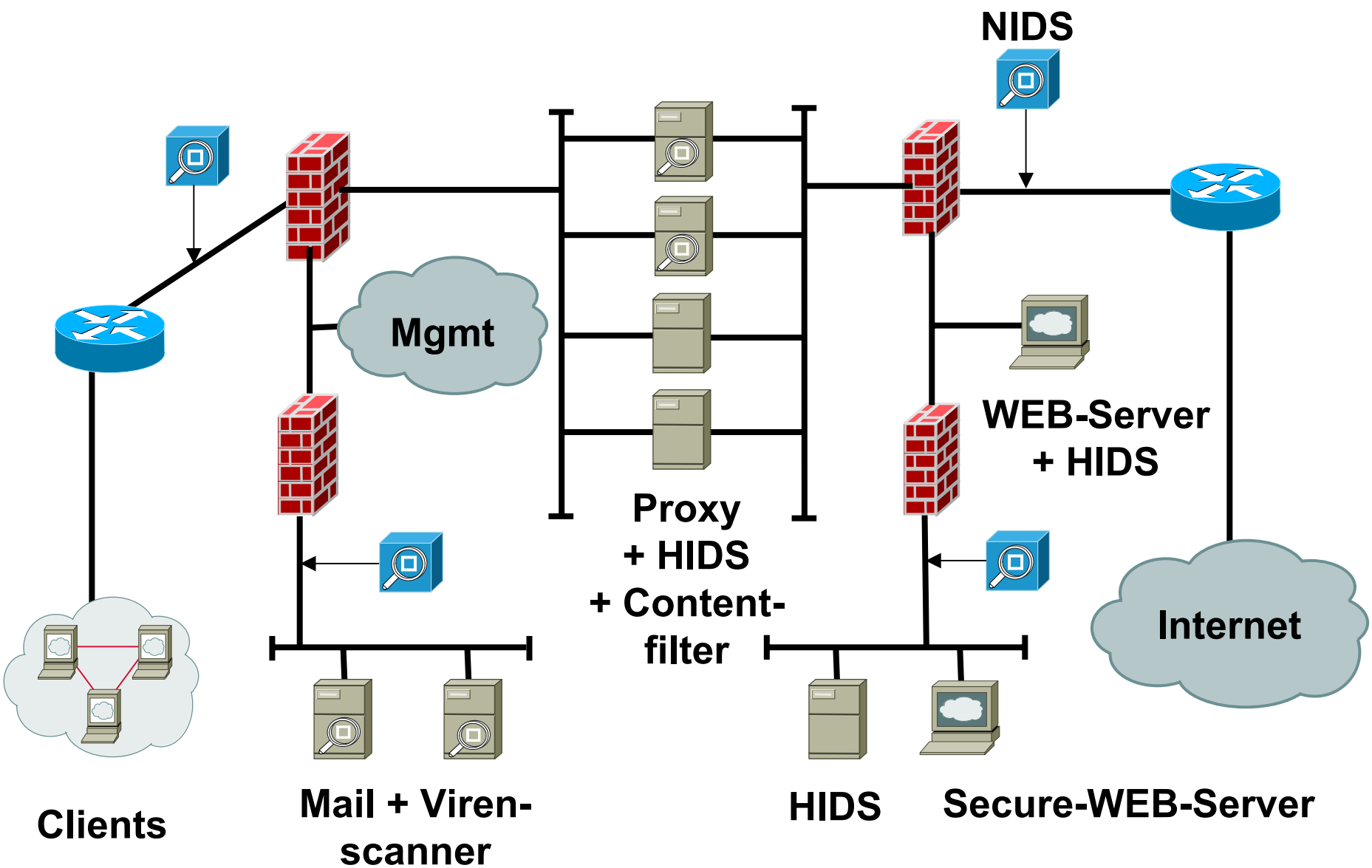
z.B.

- Rechnungswesen
- Personalmanagement
- Kanzleiorganisation
- Online Services

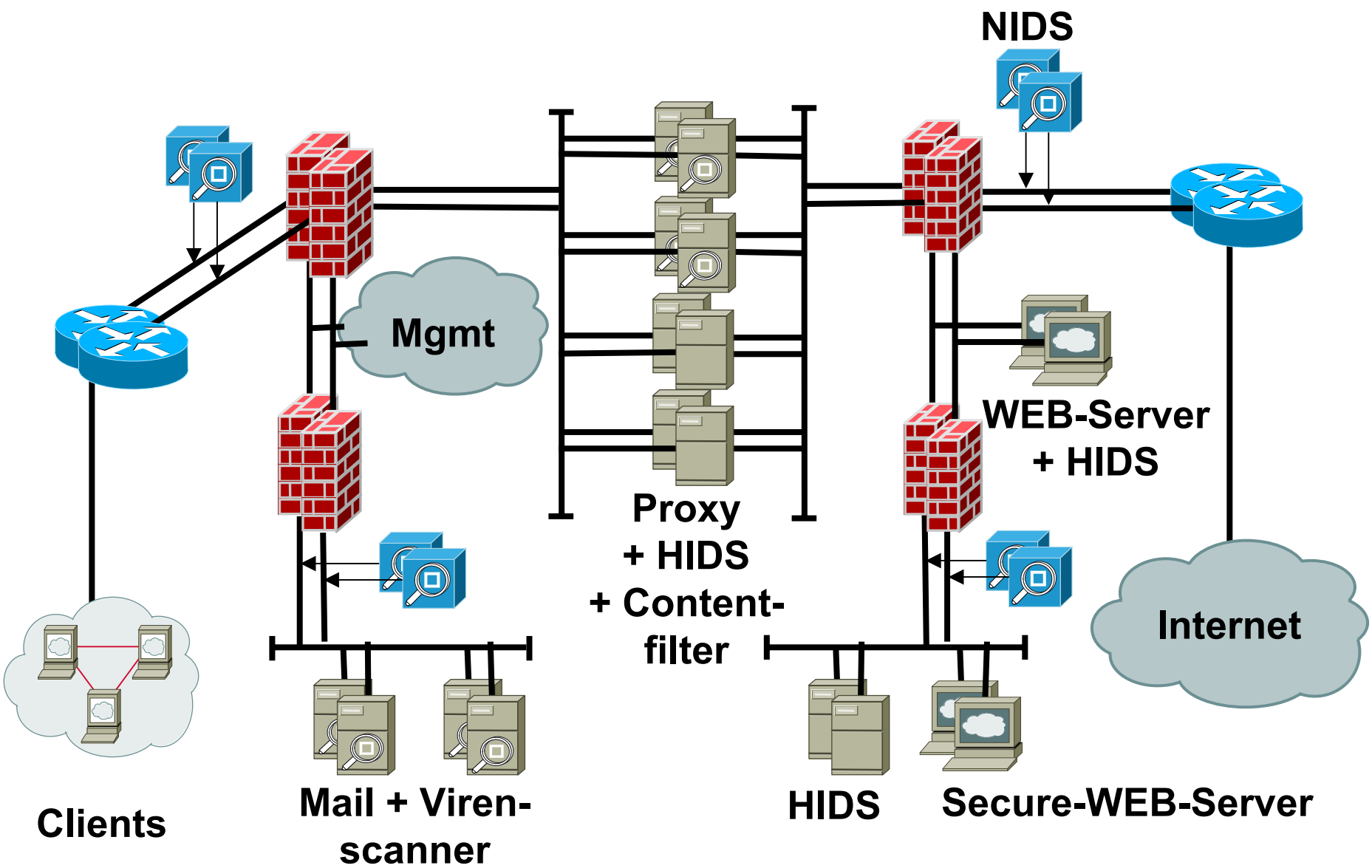
Secure Internet Provider

Auf Innovation programmiert.

Sichere Netzwerke



Sichere Netzwerke



Datenreduktion

- „Interne“ Werkzeuge
- Korrelation
  - „Gleichartige“ Meldungen zusammenfassen
  - „Unwichtige“ Meldungen unterdrücken
- Alarmierung
- Softwaresysteme
  - IBM Risk Manager
  - ISS Site Protector mit Fusion Modul
  - Symantec SESA
  - Micromuse Netcool

Managed Security Services

- „Externe“ Werkzeuge
- 7x24x365
- Managed Security Service
  - Activis
  - Controlware
  - IBM
  - Symantec

Anforderungen ??

Anforderungskatalog

Anforderungen an MSS (1)

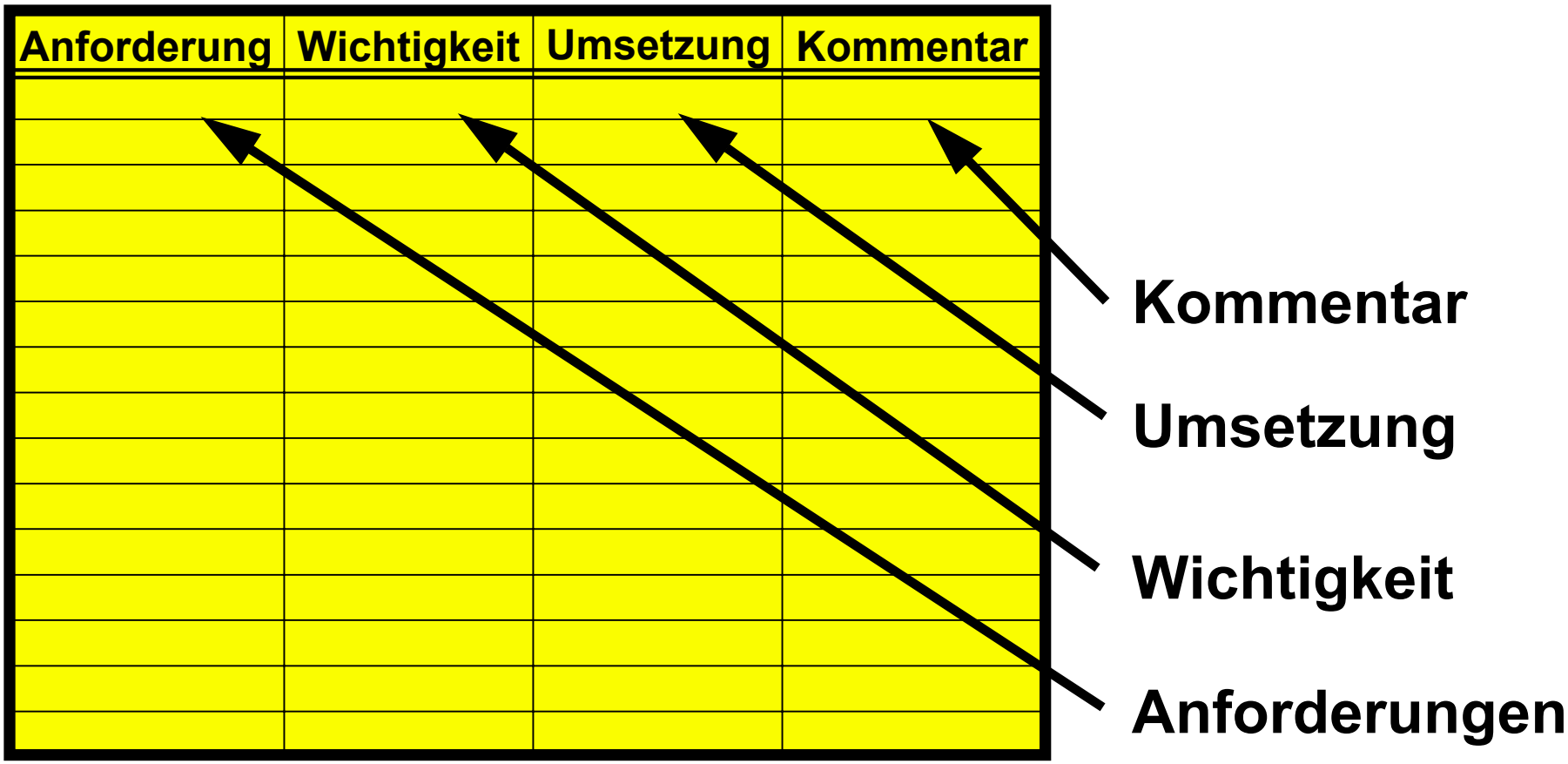
- **Voraussetzungen**
  - **Technische Gegebenheiten**
  - **Organisatorische Anweisungen**
  - **Rechtliche Aspekte**
- **Theoretische Einschränkungen**
  - **Technische Grenzen**
- **Praktische Einschränkungen**
  - **Angebote der MSS Dienstleister**

Liste mit Idealvorstellungen

Anforderungen an MSS (2)

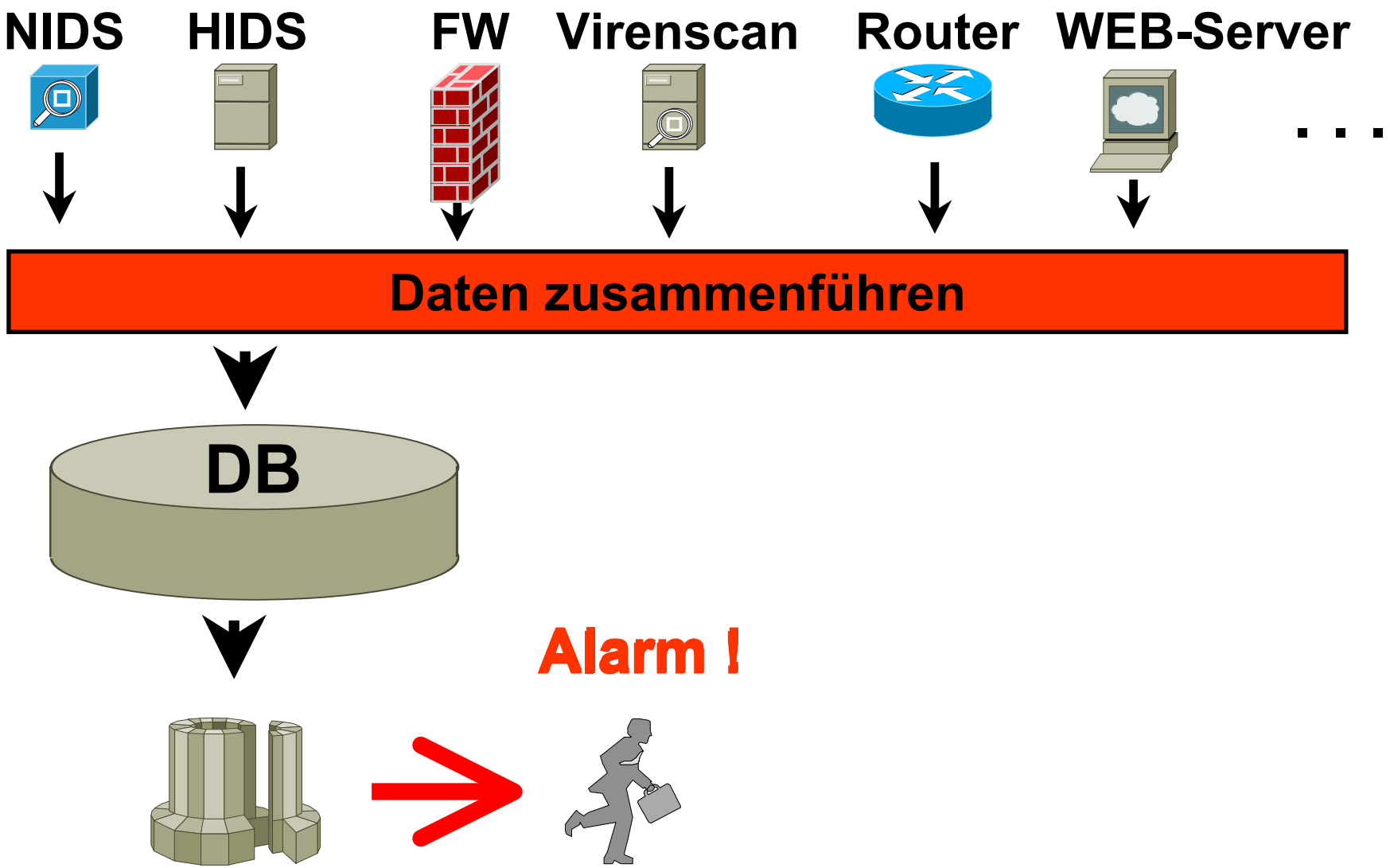
- Sicherheitsverletzungen erkennen
- Zeitnahe Reaktion
- Unterdrückung von Fehlalarmen
- Überwachung 7x24x365
- Qualifizierte Reaktion
- Korrelation der Eventquellen
- Korrelation mit Netzwerkstruktur
- Unterstützung vieler Systeme
- Flexibilität bei der Alarmierung
- Datenvertraulichkeit
- Sicherheit des MSS-Centers
- Datensicherung, Beweissicherung
- Know-how im MSS-Center
- Redundanz des MSS-Centers
- Flexible Statistiken

Anforderungen an MSS (3)

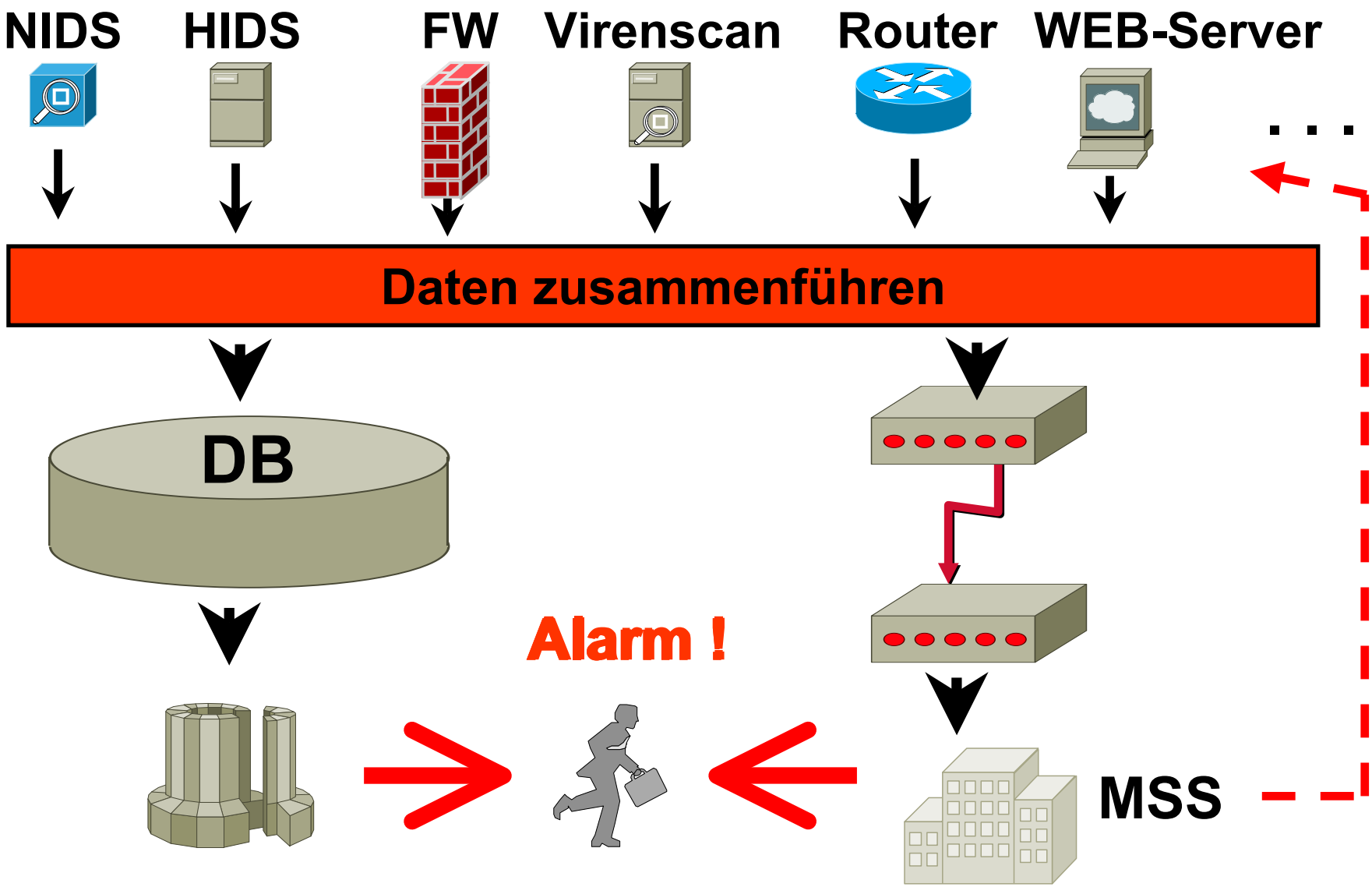


Bewertung = $\sum_{j}$ (Wichtigkeit x Umsetzung)

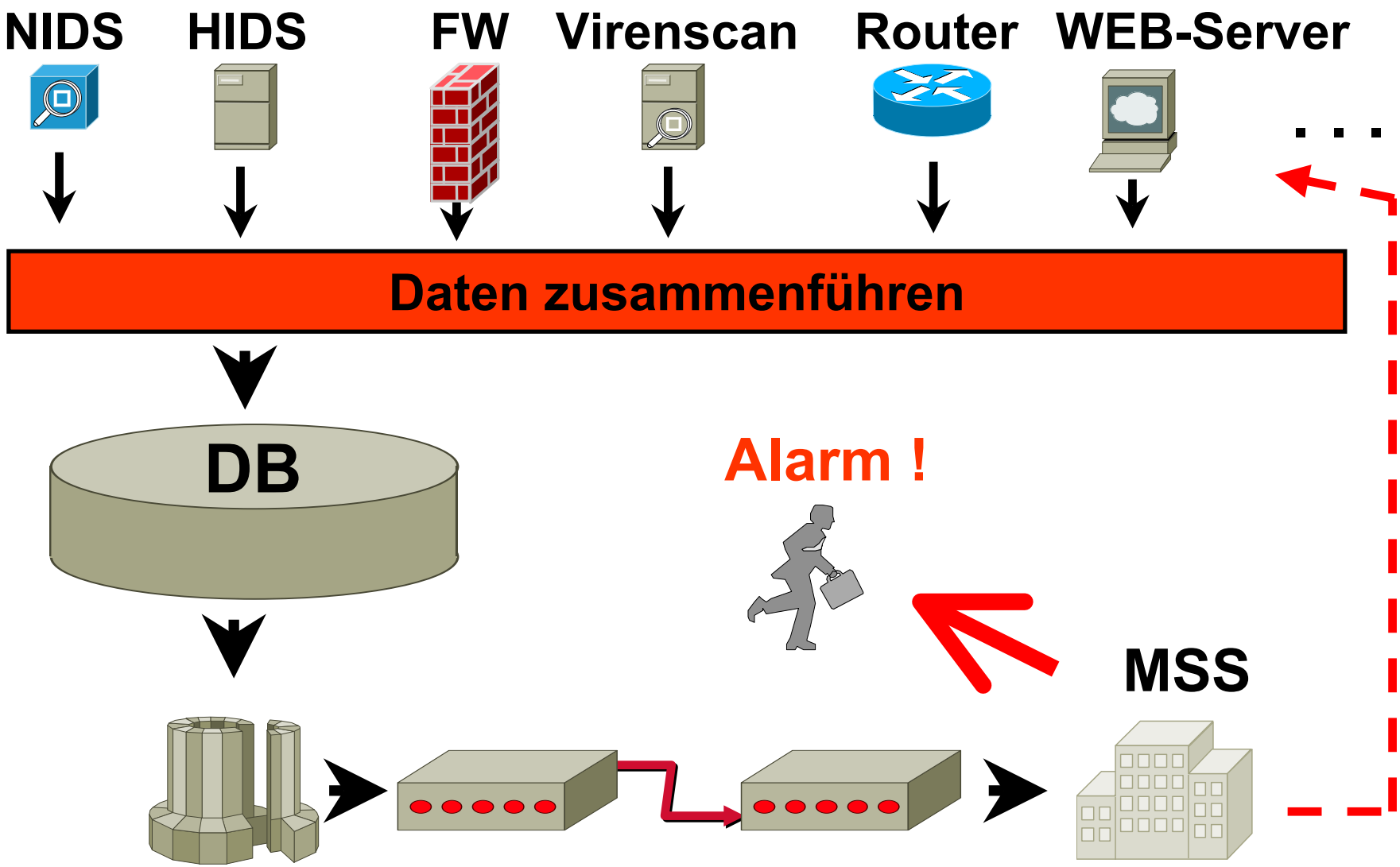
Zusammenfassung (1)



Zusammenfassung (1)

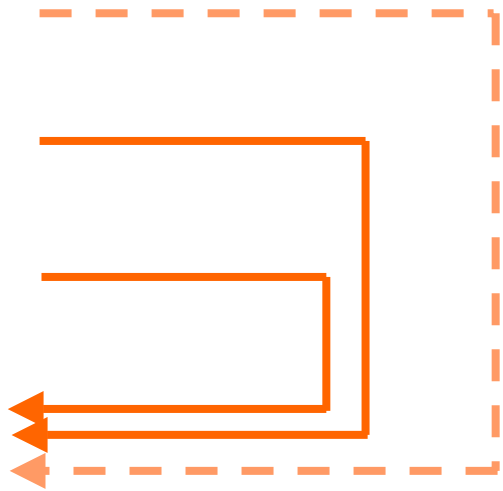


Zusammenfassung (2)

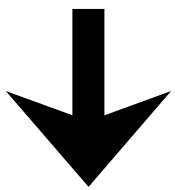


Zusammenfassung (3)

- „interne“ Lösung
- „externe“ Lösung
- „kombinatorische“ Lösung



Anforderungen an MSS



Anforderungskatalog mit Bewertung

Zusammenfassung (4)

Managed Security Service:

Die Lösung aller IT-Incident Management Probleme ?

➔ Technik + Organisation + Finanzen