



Information
Security Society
Switzerland
> *vormals FGSec*

Threat Modeling in Security Architecture

-- **Bedrohungsmodellierung in der Sicherheitsarchitektur**

30.9.2008, SAS Hotel Radisson, Luzern

ISSS Security Architecture Working Group

Tobias Christen, Beatrice Gruber, Roland Portmann, Lukas Ruf, Anthony Thorn

Speaker: Dr. Lukas Ruf, Consecom AG

Consecom AG



ICT Security and Strategy Consulting

Agenda

- Risikodefinition und Modellierung
- Zielsetzung der ISSS Working Group Security Architecture
- Bedrohungsmodellierung
- Eigenschaften des Modells
- Anwendung
- Zusammenfassung und Schlussfolgerung

Risikodefinition nach ISO

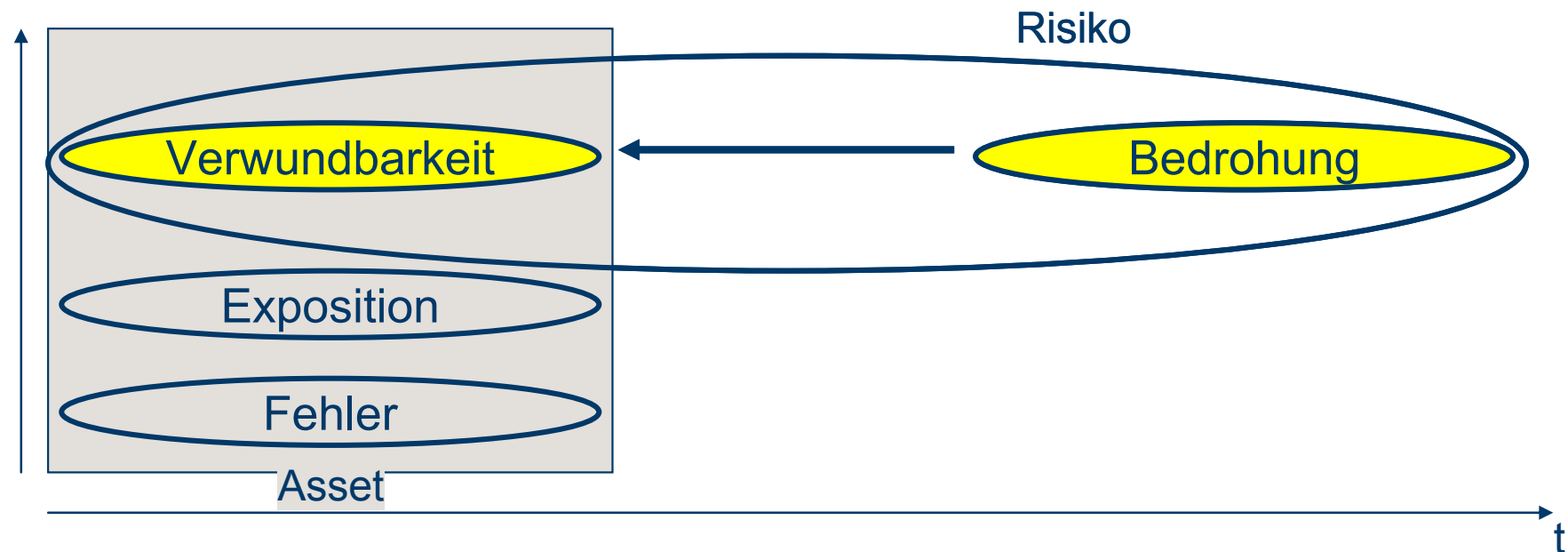
Definition

- **[ISO 13335-1:1996]. ISO/IEC 21827: 2002-10-01**
The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

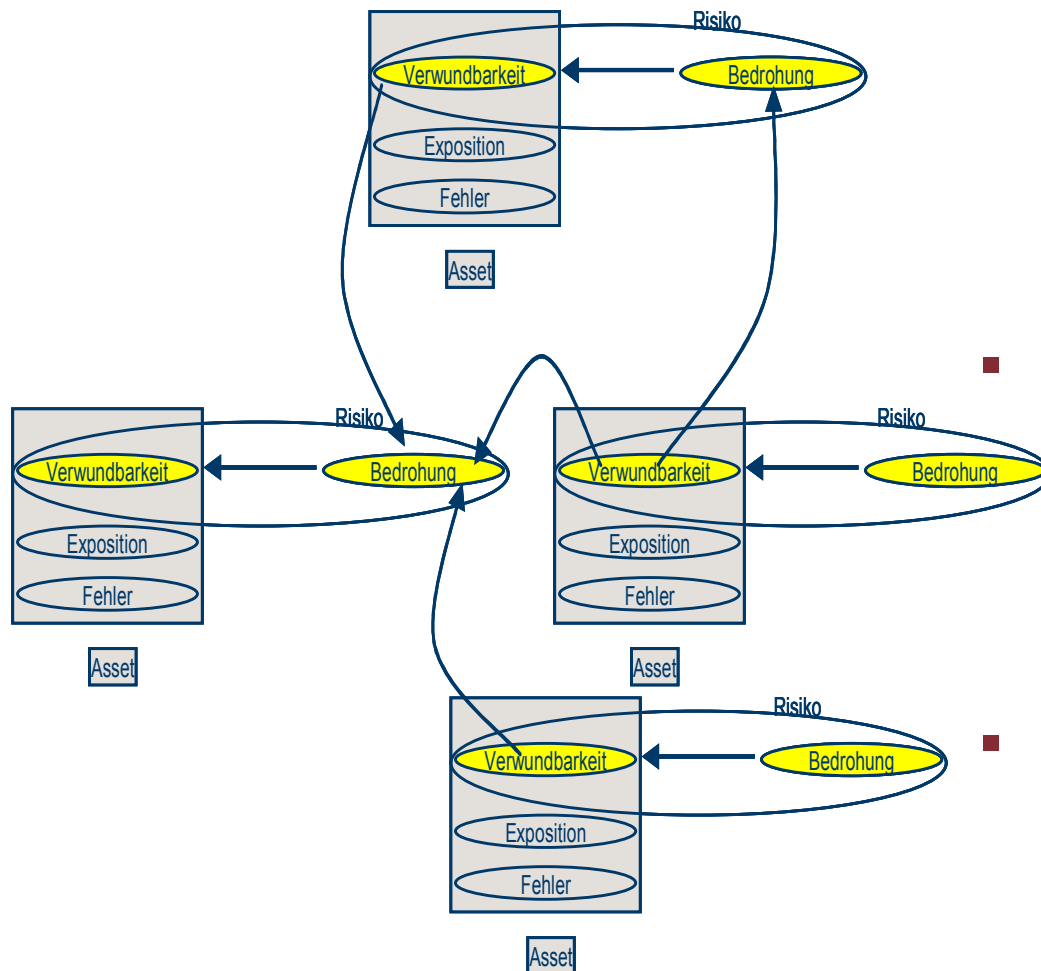
■ Quantifizierung

- Risiko(Asset, Verwundbarkeit, **Bedrohung**) =
||Auswirkung(beeinträchtigt Asset) *
Eintrittswahrscheinlichkeit(Verwundbarkeit(Asset),
Bedrohung) ||

Risikomodellierung visualisiert



Bedrohungen durch Beeinträchtigungen anderer Assets



- Bedrohungen
 - Resultieren häufig aus Beeinträchtigungen anderer Assets
 - Bilden ein Netz von direkten und indirekten Bedrohungen
- Analyse der Bedrohungsexponiertheit
 - Erfordert ein umfassendes Verständnis der Verwundbarkeiten und Abhängigkeiten
- Verlangt ein systematisches Vorgehen

Zielsetzung der ISSS AG Security Architecture

- Analyse der fundamentalen Eigenschaften von Bedrohungen
 - Strukturierung der Bedrohungseigenschaften
- Verbesserung des Basis-Verständnis von Bedrohungen
- Unterstützung der Bedrohungsanalyse

Bedrohungsmodellierung

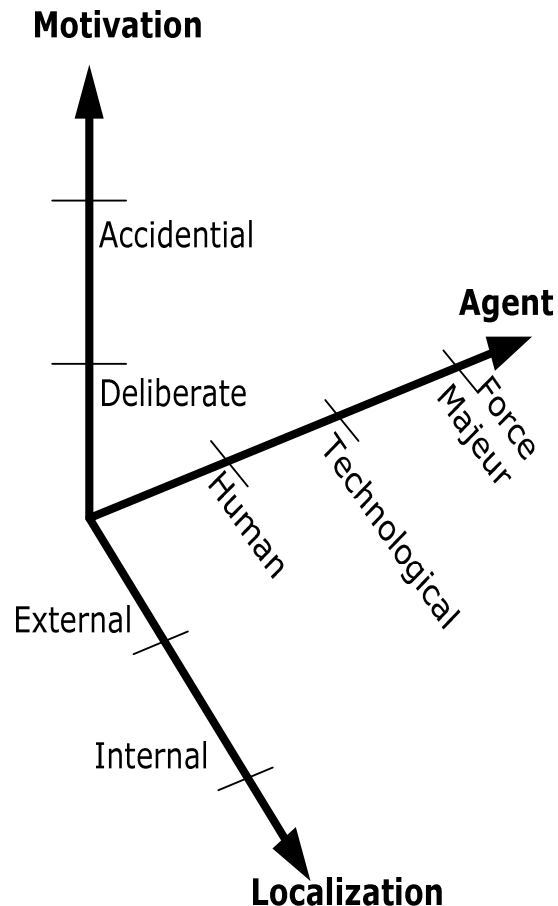
Motivation

- Klare Unterteilung
- Verbessert das Verständnis
- Unterstützt den Analysten

Modelleigenschaften

- Einteilung der Bedrohungen
 - Bedrohungen erster Ordnung
 - "Primäre Ursache"
 - Bedrohungen höherer Ordnung
- Orthogonale Strukturierung
 - Bedrohungen erster Ordnung
 - Definition der grundlegenden Eigenschaften

Orthogonales Modell für Bedrohungen erster Ordnung



- Raum von Bedrohungen
 - 3 Dimensionen
 - Motivation
 - Agent
 - Lokalisation
- Klare Einteilung durch Orthogonalität
- Basis für Vergleichbarkeit
- Grundlage für systematisches Vorgehen

Bedrohungsdimension Lokalisation

■ Lokalisation

■ Extern

z.B.

- Angreifer
- Umsysteme
- Wetter

■ Beispiel

- Ein Hacker greift ein System von ausserhalb an.

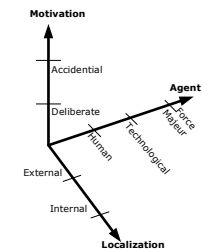
■ Intern

z.B.

- Mitarbeiter
- Schaltungen
- Wassereinbruch

■ Beispiel

- Ein Mitarbeiter löscht Daten.



Bedrohungsdimension Agent

■ Agent

■ Mensch

z.B.

- in persona
- Gesetze, Richtlinien

■ Technologie

z.B.

- Chemische Reaktionen
- Versagen
- Fehlfunktionen

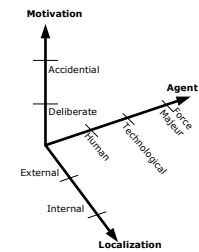
■ Höhere Macht

z.B.

- Wind & Wetter
- Erdbeben

■ Beispiele

- Ein Alterungsprozess bedingt, dass eine Schaltung plötzlich nicht mehr korrekt funktioniert.
- Wind lässt einen Baum auf ein Fahrzeug fallen.



Bedrohungsdimension Motivation

■ Motivation

■ Mutwillig/Vorsätzlich

z.B.

- Einfügen von Fehlern
- Zerstörung
- Vandalismus

■ Beispiel

- Programmierer fügt eine Schwachstelle für Spionagezwecke in Software ein.

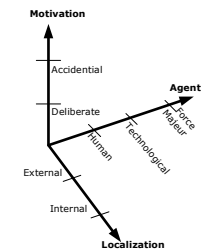
■ Zufällig

z.B.

- Zerstörung durch Unachtsamkeit
- Fehler durch Missverständnisse

■ Beispiel

- Ein Erdbeben reißt eine Hochspannungsüberlandleitung runter.



Intention wird nur den Menschen (Dimension *Agent*) zugestanden

Anwendung des Bedrohungsmodells

- Unterstützt systematische Vorgehensweise bei der Bedrohungsanalyse
- Vereinheitlichte Darstellung der Bedrohungslage
 - Bedrohungsraum mit Unterräumen
- Ermöglicht Vergleichbarkeit
 - Bedrohungsvektoren:
 - [Lokalisation, Agent, Motivation]

Zusammenfassung und Schlussfolgerung

- Bedrohungen sind für die Risikoanalyse zentral.
 - Direkte Bedrohungen
 - Direkte Auswirkungen auf ein Asset
 - Indirekte Bedrohungen
 - Der Beeinträchtigung eines Assets wird zur Bedrohung für ein nachfolgendes.
- Bedrohungsmodellierung der ISSS AG Security Architecture
 - Einteilung in Bedrohungen erster und höherer Ordnung
 - Orthogonalität bei Bedrohungen erster Ordnung
 - Dreidimensionales Modell
 - Lokalisation
 - Motivation
 - Agent
 - Erlaubt Strukturierung des Bedrohungsraumes
 - Das Konzept kann auf Bedrohungen höherer Ordnung angewendet werden.
- Fördert das Verständnis der Bedrohungsexponiertheit
- Unterstützt die Risikoanalyse



Information
Security Society
Switzerland
> *vormals FGSec*

ISSS Security Architecture Working Group

Tobias Christen, Beatrice Gruber, Roland Portmann, Lukas Ruf, Anthony Thorn

Speaker: Dr. Lukas Ruf, Consecom AG

Consecom AG



ICT Security and Strategy Consulting