



# OWASP AppSec Germany 2010

**OWASP**

20.10.2010

**Sebastian Klipper**

**Ps(i)<sup>2</sup> – Sicherheit in Informationssystemen**

owasp@psi2.de

<https://psi2.de>

Copyright © The OWASP Foundation

Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

**The OWASP Foundation**

<http://www.owasp.org>

Sebastian Klipper

# Konfliktmanagement für Sicherheitsprofis

Auswege aus der „Buhmann-Falle“ für IT-Sicherheitsbeauftragte, Datenschützer und Co

PRAXIS

<kes>



Sebastian Klipper

# Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005 und 31010

PRAXIS



# Sebastian Klipper

Ps(i)<sup>2</sup> - Sicherheit in Informationssystemen

Information Security Consultant  
und Fachbuchautor  
aus Berlin





Fehlt die  
**Kompetenz**  
auf OSI-Layer 8?



Anwendungsschicht	7
Darstellungsschicht	6
Sitzungsschicht	5
Transportschicht	4
Vermittlungsschicht	3
Sicherungsschicht	2
Physikalische Schicht	1





Der Mensch steht  
im Mittelpunkt





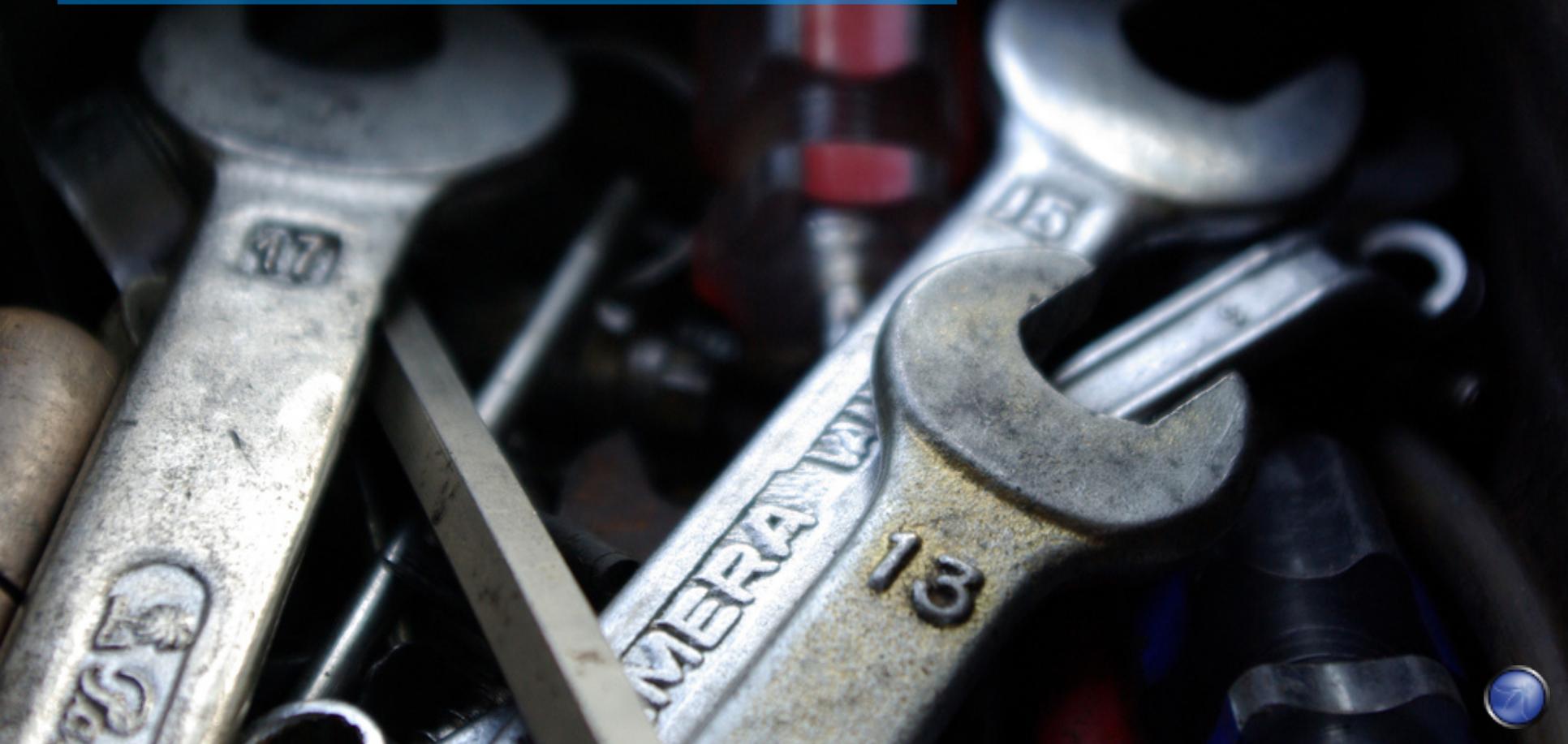
**Zwänge** Ziele  
Prioritäten **Risiken**



Technik  
ist nicht **Alles**



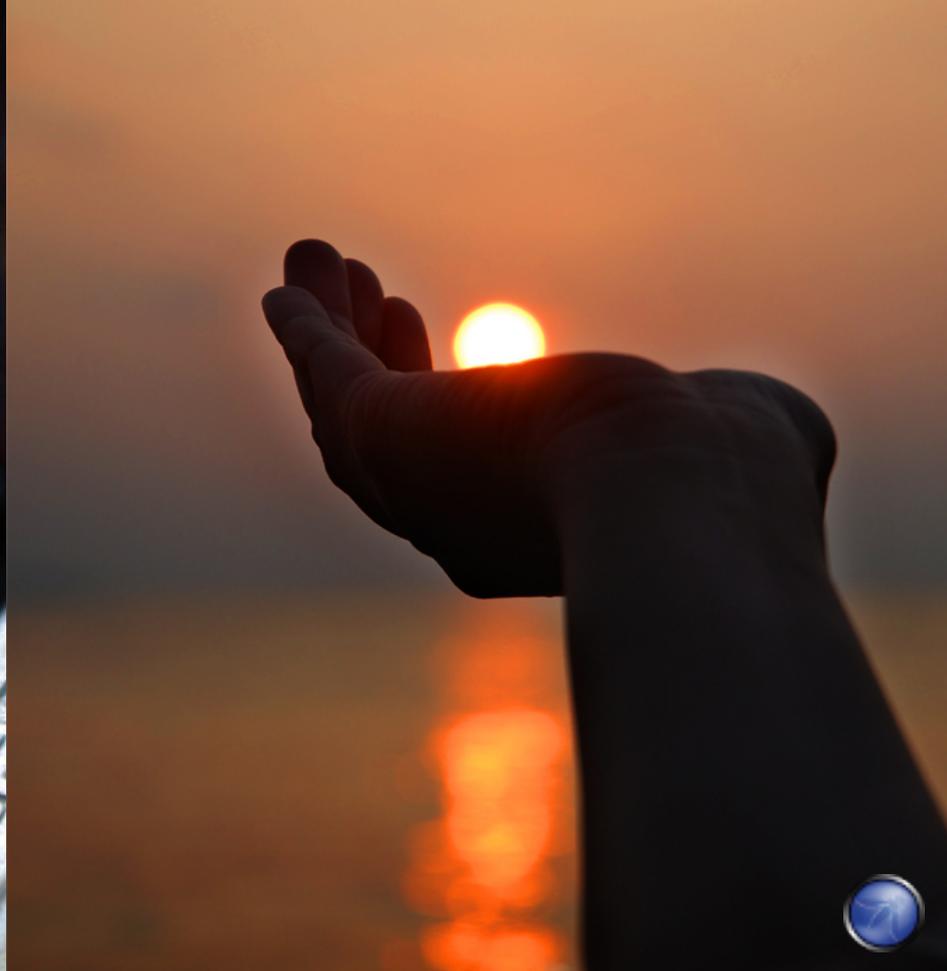
Warum  
benutzen  
**Menschen**  
Werkzeuge?



Muss sich **das Werkzeug**  
an den **Menschen**  
**anpassen...**



...oder der **Mensch**  
an das  
**Werkzeug?**





Was sind die  
richtigen  
**Fragen?**





**Mensch**  
oder  
**Fotoapparat?**





Fehlt die  
**Kompetenz**  
*auf* oder *für* OSI-Layer 8?







# Fischen im Trüben?



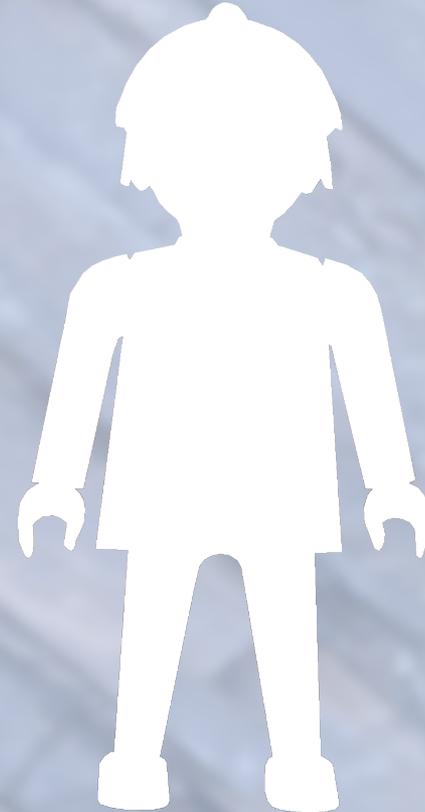
# Informations-und Kommunikations- Technik



Sender

← Nachricht →

Empfänger



Kommunikation



Sender

← Nachricht →

Empfänger



Kommunikation

Sender

← Nachricht →

Empfänger



Kommunikation

Sender

← Nachricht →

Empfänger



Kommunikation

Sender

← Nachricht →

Empfänger



Kommunikation





# Visuelle Kommunikation



**Ein Beispiel:**  
Was nicht  
**passt...**



**Apps**

**Add-ons**

**Plug-ins**



**Widgets**

**Sicherheitsprobleme**  
durch Erweiterungen



**Werkzeug:**  
**Ein Hammer**





Mit Schraub-**Plug-in**:  
Der **Schrammer**



Mit Zangen-Add-on:  
Der Zangschrammer



Mit Bleistift-Widget:  
Der Zangbleischrhammer



Mit Feierabend-App:  
Der Zangbleischrammzieher



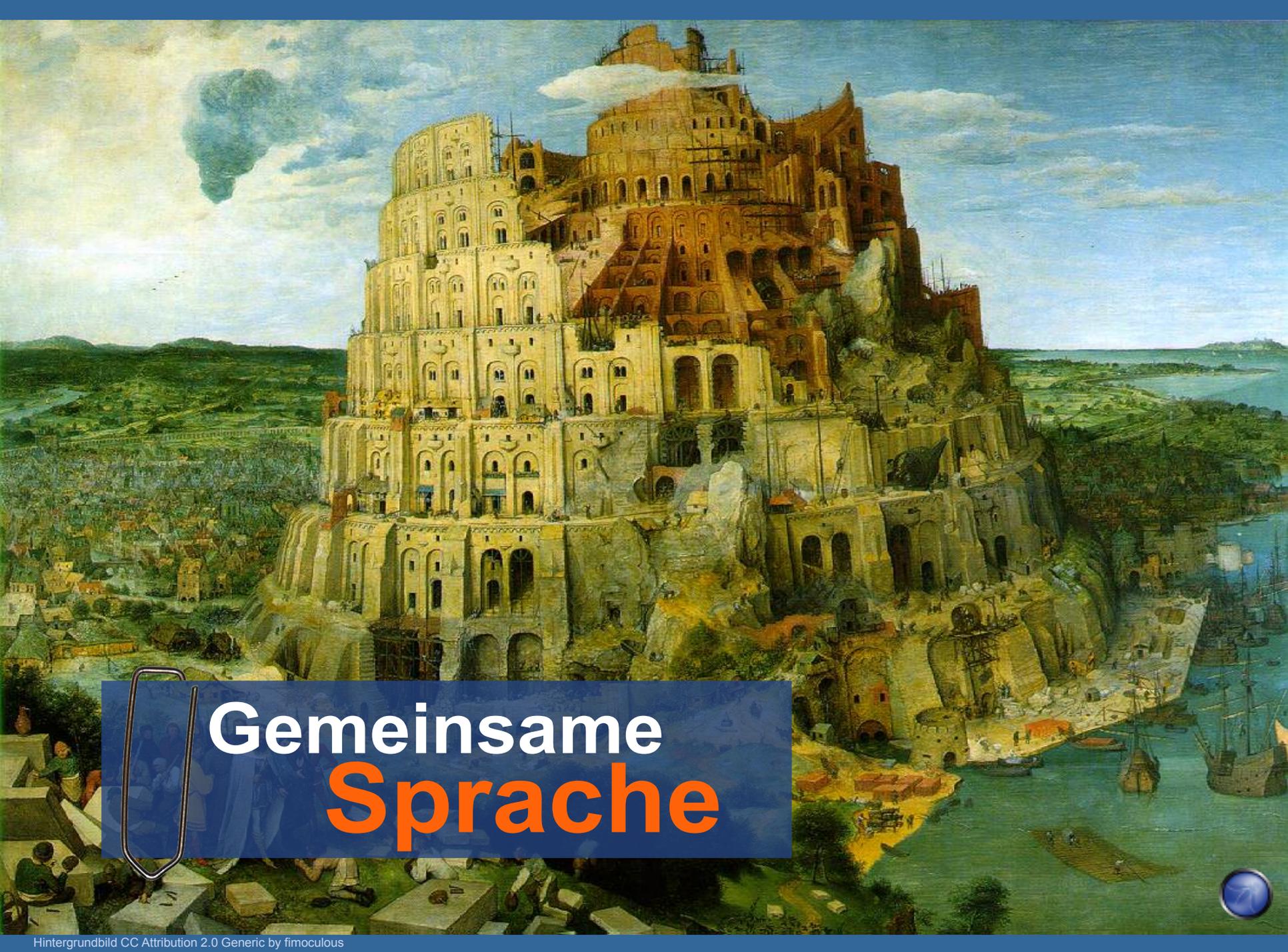
Sichere Multitools gibt es nicht zum

**Nulltarif...**



...und Erweiterungen  
**brauchen Zeit**





# Gemeinsame Sprache





Sicherheit muss  
ver**MARKT**et  
werden





**Zwänge** Ziele  
Prioritäten **Risiken**





Wir brauchen mehr  
**Kompetenz**  
für OSI-Layer 8!





# OWASP

AppSec Germany  
20.10.2010 

Die führende deutsche Konferenz zur Web Application Security in Nürnberg.



# OWASP AppSec Germany 2010

**OWASP**

20.10.2010

**Sebastian Klipper**

**Ps(i)<sup>2</sup> – Sicherheit in Informationssystemen**

owasp@psi2.de

<https://psi2.de>

Copyright © The OWASP Foundation

Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

**The OWASP Foundation**

<http://www.owasp.org>