



OWASP Top 10 – Was t/nun?

OWASP

Nürnberg, 20.10.2010

Dirk Wetter

Dr. Wetter IT-Consulting & -Services

mail bei drwetter.punkt.eu

dirk.punkt.wetter@owasp.punkt.org

+49-(40)-2442035-1

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>

C'est moi

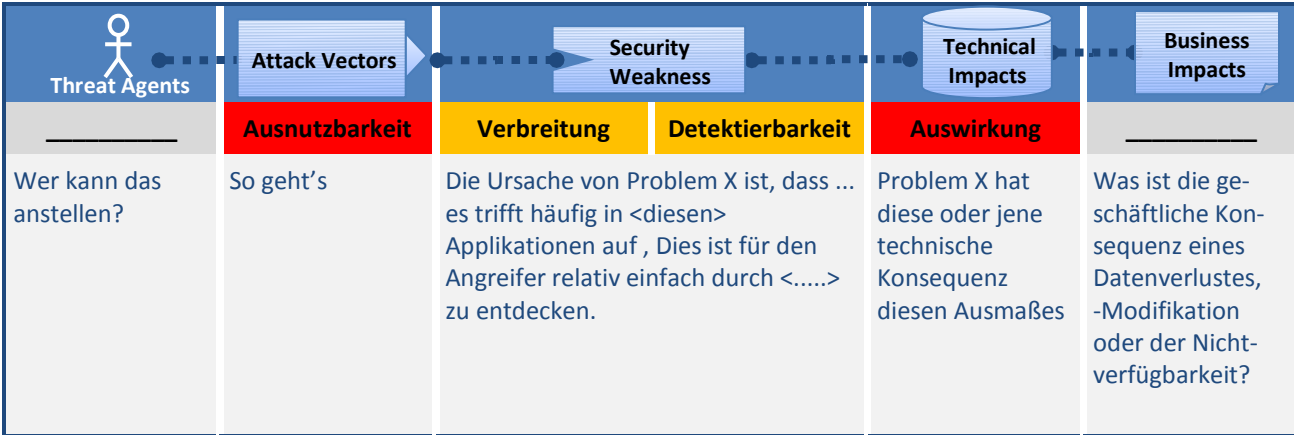
- Selbständig, IT-Sicherheitsberatung
- Engagiert in GUUG: Vorstand, Konferenzen
- Bissertl auch in OWASP
- Vom Herzen Unixer seit > 2 Dekaden
 - Netze!
 - (trotzdem kein Win-Dummy)
- Schreibe gerne

OWASP Top 10: Geschichte

- **4. Ausgabe (2003, 2004, 2007, 2010)**
- **2007:**
 - ▶ Pro „Issue“ 2-4 Seiten mit Abschnitten
 - Grundsätzliche Infos
 - Environments Affected (Ist das ein spezieller Fehler?)
 - Vulnerability (Erklärung)
 - Verifying Security (Wie kann ich's feststellen?)
 - Protection
 - Samples (Links nach cve.mitre.org)
 - References

Kausalkette
Bedrohung ... Auswirkung

A# Problem X



Bin ich verwundbar für diese Schwachstelle?

The best way to find out if an application is vulnerable to the according problem #X is

Wie kann ich's verhindern?

1. So and so
2. But I would try this too
3. And this is not bad either

Beispiel: Angreiferszenario

One line of stupid example (code) here

<http://howtoexploit-this-stupid.code>

References

OWASP
(Test./Dev. Guide, ASVS, ESAPI,...)

External
CWE meistens



Facts first

- **2010**
 - ▶ Kürzer: 35 vs. 22 Seiten (!)
 - Unter'n Tisch gefallen:
 - Sprachspezifische Empfehlungen
 - Kritiker: Weniger Ausführlich / Andere: Mehr auf den Punkt
 - Ausführlicher: Hinter Top 10 „What's Next”
 - Developers
 - Verifiers
 - Organizations
 - ▶ But most importantly...

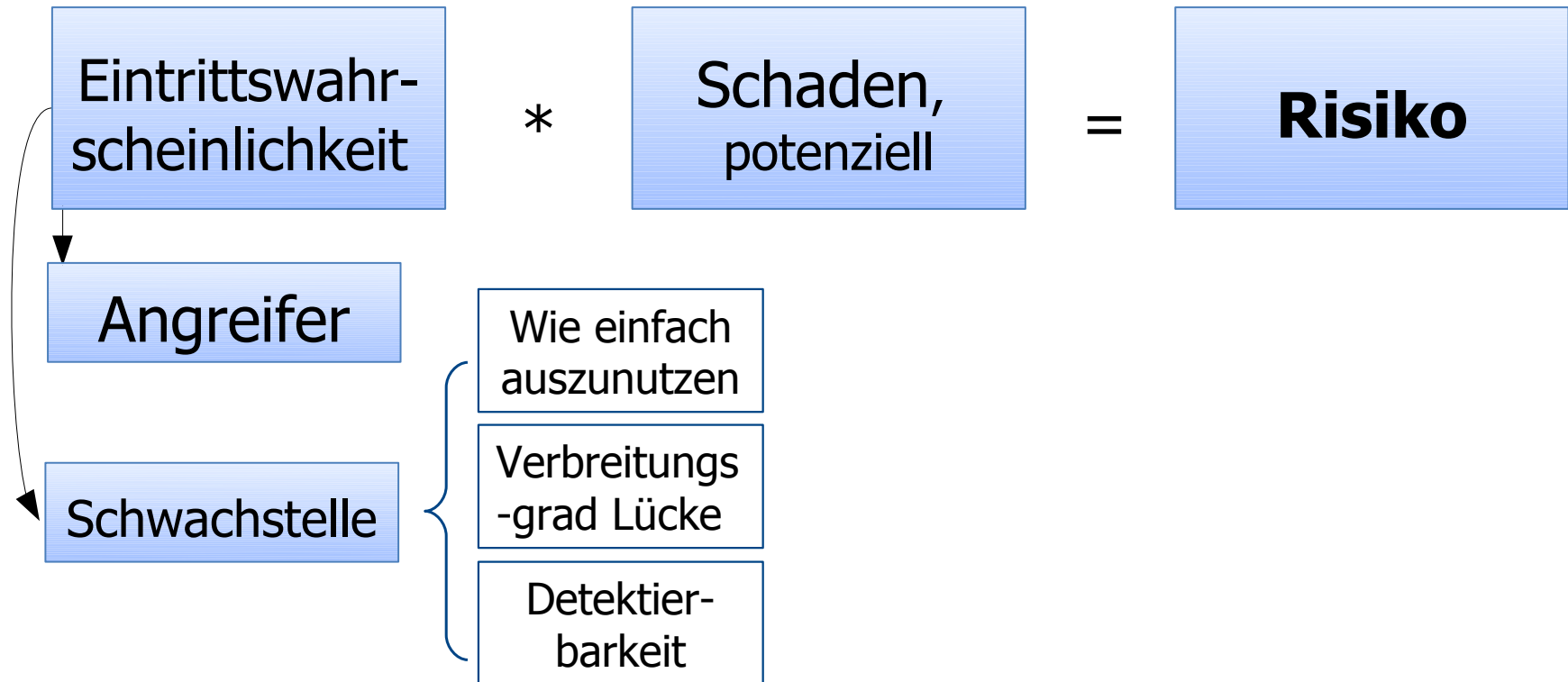
Schwachstellen vs. Risiken

- 2007 → **Schwachstellen**
 - ▶ webbezogene MITRE Vulnerability Trends aus 2006
- 2010 → **Risiken**
 - ▶ Goal: Awareness AppSec Risks
 - ▶ 2 Extra-Seiten am Ende
 - ▶ Warum wichtig?
- Erste Linie:
 - ▶ ist das Risiko fürs Geschäft und nicht die Technik
 - ▶ Allerdings Businessrisiko
 - firmenspezifisch, kann OWASP nicht klären

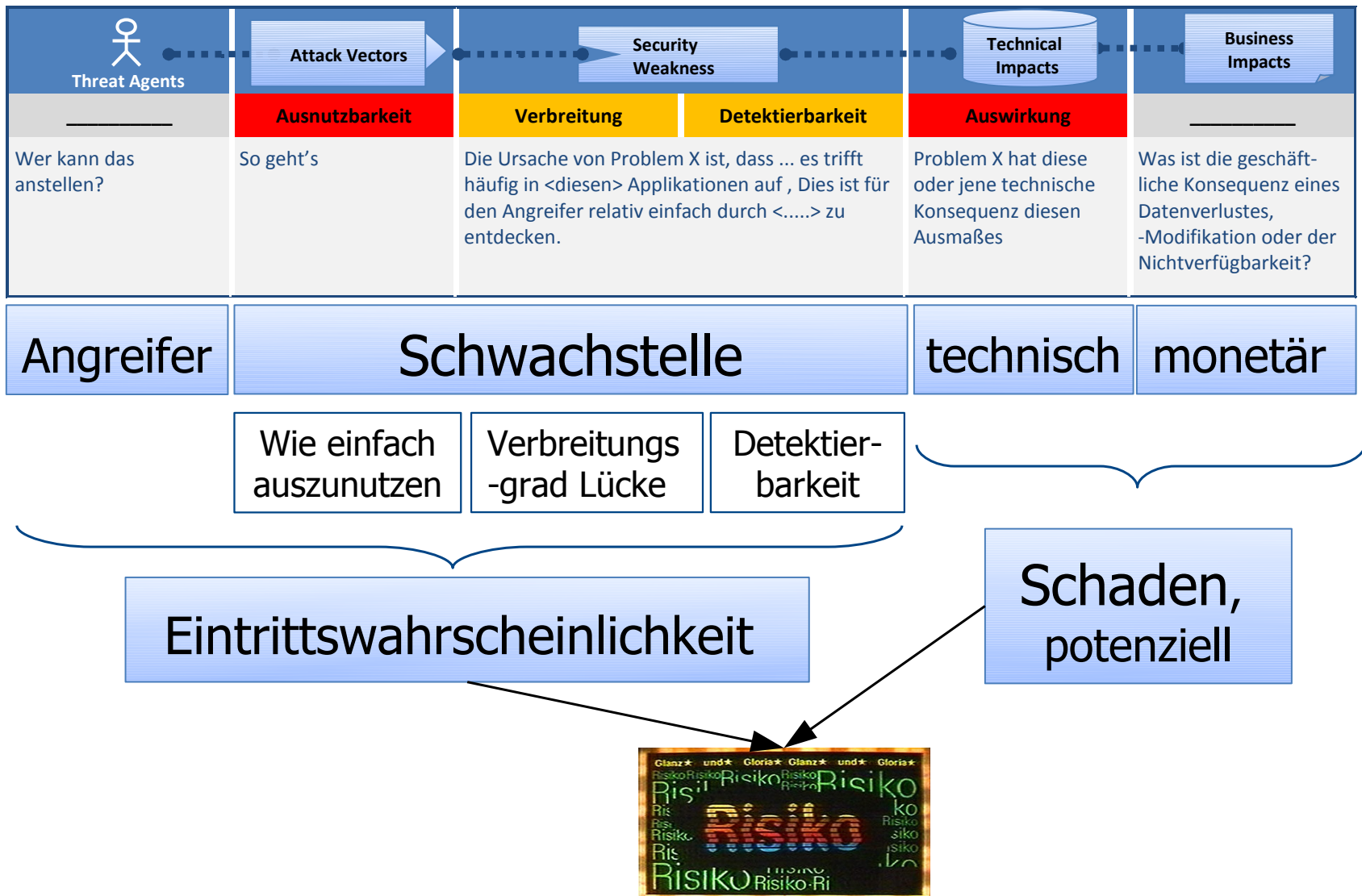


It's all about Risk

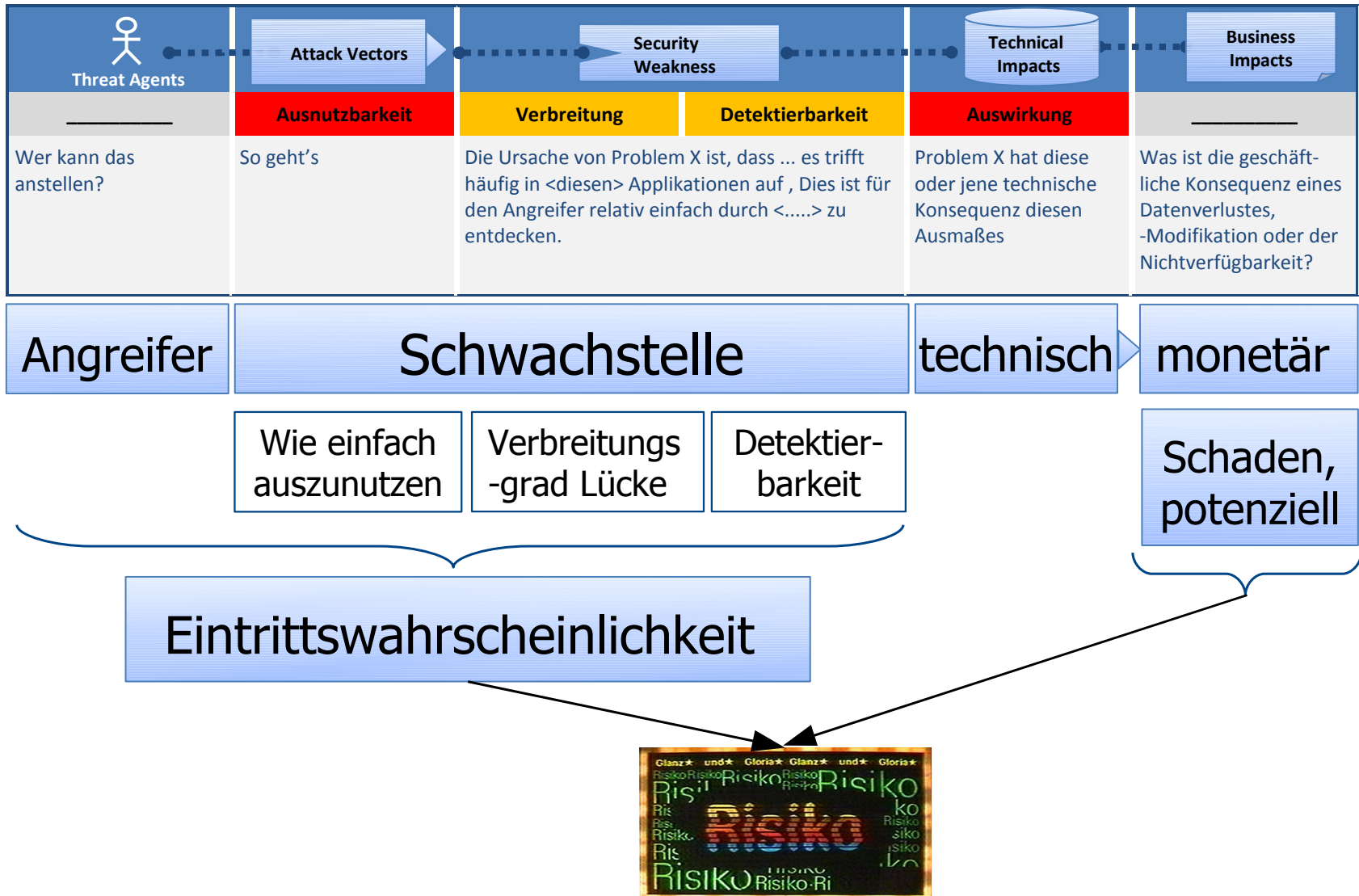
- Wo kommt's her?
 - OWASP Testing Guide v3, da drin:
 - OWASP Risk Rating Methodology



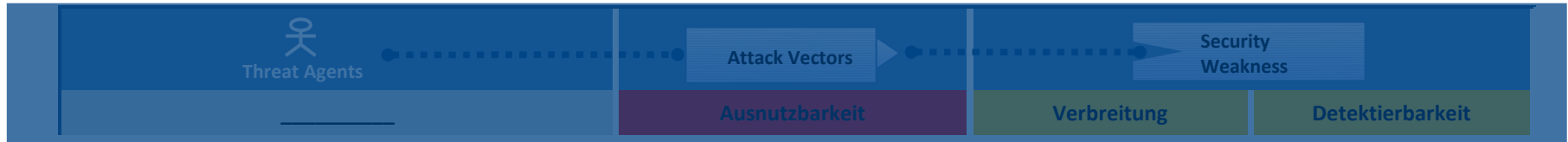
It's all about Risk



It's all about Risk



Rate it!: Eintrittswahrscheinlichkeit



Angreifer

| | | | |
|-----------------------|----------------|----------------------|----------------|
| Größe Gruppe (1-9) | Motiv (1-9) | Gelegenheit (1-9) | Skill (1-9) |
|-----------------------|----------------|----------------------|----------------|

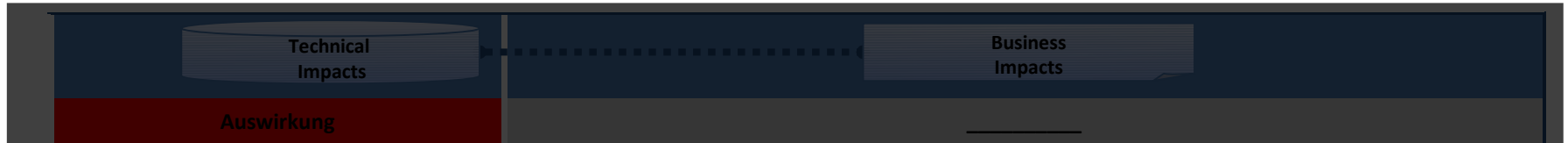
Schwachstelle

| | | |
|-------------------------|-------------------------|----------------------------|
| Wie einfach auszunutzen | Verbreitungs-grad Lücke | Detektier-barkeit |
| Theoretisch (1) | (1) | Kaum (1) |
| Schwierig (3) | (3) | Schwierig (3) |
| Einfach (5) | (4) | Einfach (7) |
| Mittel autom. Tools (9) | (6) | autom. Tools verfügbar (9) |
| | (9) | |

Zahl | Zahl | Zahl | Zahl | Zahl | Zahl | Zahl

Ø (Zahlen) = Eintrittswahrscheinlichkeit

Rate it!: Schaden



| technisch | | | | | monetär | | | |
|--------------------------------------|------------------|---------------------|--------------------------|--|----------------------|------------|------------|---------------|
| Verlust von | | | | | Finanzieller Schaden | Reputation | Compliance | Datenverlust |
| Vertraulichkeit (1-9) | Integrität (1-9) | Verfügbarkeit (1-9) | Rückverfolgbarkeit (1-9) | | << Fixen (1) | (1) | (2) | Für einen (1) |
| | | | | | << Gewinn p.A. (3) | (4) | (5) | Hunderte (3) |
| | | | | | Signifikant (5) | (5) | | Tausende (7) |
| | | | | | Insolvenz (9) | (9) | (7) | Millionen (9) |
| Zahl Zahl Zahl Zahl | | | | | Zahl | Zahl | Zahl | Zahl |

∅ (Zahlen) = potenzieller Schaden



Risikograph

| Risiko über alles | | | | |
|----------------------|--------------------|-------------------|--------------------|-------------|
| Schaden (potenziell) | Hoch > 6 | Mittel | Hoch | Kritisch |
| | Mittel 3 - 5.99 | Niedrig | Mittel | Hoch |
| | Niedrig < 2.99 | Info | Niedrig | Mittel |
| | | Niedrig < 2.99 | Mittel 3 - 5.99 | Hoch > 6 |
| Wahrscheinlichkeit | | | | |

- YMMV!
 - ▶ Siehe z.B. Rating für Insolvenz
 - ▶ Wichtung erwägen

Risiko: Wozu nun das Ganze?

- Risikomanagementprozess:
 - ▶ Erfassung
 - Analyse: Code / externer Audit
 - Bewertung darin: Conditio sine qua non
 - ▶ Steuerung
 - ▶ Kontrolle
- Technisch: Strukturiert und priorisiert fixen
- Business: Rechte Balance zw. Geld und Sicherheit
- Mehr? ISO 27005, BS 31100:2008, BSI 100-3,
 - ▶ [OWASP Threat Risk Modelling](#)

| | 2010 | 2007 |
|------------|--|--|
| A1 | Injection Flaws | Cross Site Scripting |
| A2 | Cross Site Scripting | Injection |
| A3 | Broken Authentication + Session Mgmt | Malicious File Execution |
| A4 | Insecure Direct Object References | Insecure Direct Object References |
| A5 | Cross Site Request Forgery | Cross Site Request Forgery |
| A6 | Security Misconfiguration <i>NEU!</i> | Information Leakage and Improper Error Handling |
| A7 | Insecure Cryptographic Storage | Broken Authentication + Session Mgmt |
| A8 | Failure to Restrict URL Access | Insecure Cryptographic Storage |
| A9 | Insufficient Transport Layer Protection | Insecure Communications |
| A10 | Unvalidated Redirects and Forwards <i>NEU!</i> | Failure to Restrict URL Access |

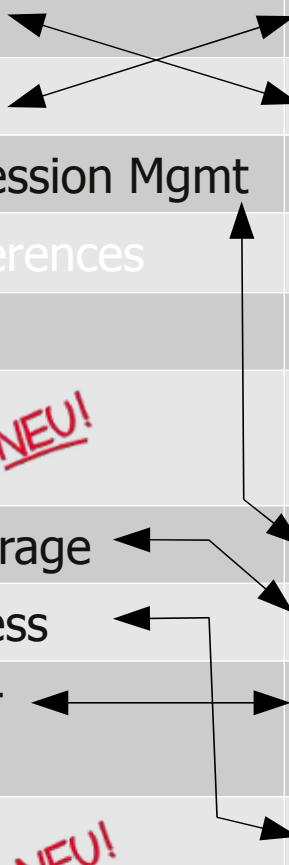


| | 2010 | 2007 |
|------------|--|--|
| A1 | Injection Flaws | Cross Site Scripting |
| A2 | Cross Site Scripting | Injection |
| A3 | Broken Authentication + Session Mgmt | Malicious File Execution |
| A4 | Insecure Direct Object References | Insecure Direct Object References |
| A5 | Cross Site Request Forgery | Cross Site Request Forgery |
| A6 | Security Misconfiguration <i>NEU!</i> | Information Leakage and Improper Error Handling |
| A7 | Insecure Cryptographic Storage | Broken Authentication + Session Mgmt |
| A8 | Failure to Restrict URL Access | Insecure Cryptographic Storage |
| A9 | Insufficient Transport Layer Protection | Insecure Communications |
| A10 | Unvalidated Redirects and Forwards <i>NEU!</i> | Failure to Restrict URL Access |



NEU!

NEU!



▪ 2007s A3 Malicious File Inclusion: RFI

- ▶ Kritik von Ryan Barnett
- ▶ Laut [zone-h](#) (hochger. Q1 2010 Statistiken):
 - 2008 < 2009 < 2010

| Attack Method | 2008 | 2009 | 2010 |
|--|--------|--------|---------|
| File Inclusion | 90.801 | 95.405 | 115.574 |
| SQL Injection | 32.275 | 57.797 | 33.920 |
| Access credentials through MITM attack | 37.526 | 7.385 | 1.005 |
| Other Web Application bug | 36.832 | 99.546 | 42.874 |
| Web Server intrusion | 8.334 | 9.820 | 7.400 |
| URL Poisoning | 5.970 | 6.294 | 3.516 |
| Web Server external module intrusion | 4.967 | 2.265 | 1.313 |



Blick über den OWASP-Tellerrand

- **SANS/CWE**



Top 25 Most Dangerous Software Errors

- ▶ Weaknesses!

- ▶ Ranking: MITRE

wie bei OWASP T10 2007

- Gut strukturiert

- Top 25 eine Seite (ok...)

- Mit Verweis auf jeweiligen CWE

<http://cwe.mitre.org/data/definitions/<zahl>.html>

- Ausführlicher: [PDF](#) 62 Seiten

- ▶ Verschiedene Ziele



Top 25 Most Dangerous Software Errors

- ▶ Jeder Punkt (Einleitung)

- Summary mit Rating

- Weakness Prevalence [Widespread,High,Common,Limited]
 - Consequences [Code execution, Data Loss, DoS, Security Bypass,..]
 - Remediation Cost [High,Medium,Low]
 - Ease of Detection [Easy,Moderate,Difficult]
 - Attack Frequency [Often, Sometimes, Rarely]
 - Attacker Awareness [High,Medium,Low]

- Discussion

- Mit Links zum CWE:

Technical Details, Code Examples, Detection Methods, References


» Dort viel Info

Top 25 Most Dangerous Software Errors

- ▶ Jeder Punkt (Hauptteil)

- Prevention and Mitigations, ggf. mehrere Punkte von:
 - Architecture and Design
 - Implementation
 - Operation
- Related CWEs
- Related Attack Patterns

Blick über den OWASP-Tellerrand

- **SANS/CWE**  **Common Weakness Enumeration**
A Community-Developed Dictionary of Software Weakness Types
Top 25 Most Dangerous Software Errors
- „Monster Mitigation Section“:
 - ▶ 5 Maßnahmen, 4 General Practices
 - ▶ Mitigation Matrix
- <http://cwe.mitre.org/top25/> bzw.
- <http://www.sans.org/top25-software-errors/>

Blick über den OWASP-Tellerrand



▪ WASC Threat Classification v2.0

- ▶ <http://projects.webappsec.org/Threat-Classification>
- ▶ 172 (!) Seiten im PDF
- ▶ 49 Punkte
- ▶ Threats = Weaknesses + Attacks



Blick über den OWASP-Tellerrand

▪ **WASC Threat Classification v2.0**



- ▶ Reference Guide für W / A
 - Out of Scope: Prevention, Detection, Threat/Risk Mgmt.
- ▶ Einzelne „Threats“ auf den Punkt gebracht
 - Codebeispiele, Erklärungen
- ▶ Kritik:
 - Stellenweise Überschneidungen
 - Struktur ist bei OWASP, SANS/CWE besser
- ▶ **Taxonomy Cross Reference View**
 - Super mapping WASC vs.
SANS/CWE vs. OWASP 2010

Blick über den OWASP-Tellerrand

- **WHID Top 10 Risks for 2010**



- ▶ DB: <http://www.xiom.com/whid/>

- ▶ (Link zur Abfrage)

- Auch ein WASC-Projekt

- ▶ Fokus eher Incidents

- Daher „nicht komplett“

- Real world!

- Und nur ausgesuchte



- ▶ Semi-Annual Report 2010

- m.W. der erste

Blick über den OWASP-Tellerrand

WHID Top 10 for 2010

- | | |
|----|--|
| 1 | Improper Output Handling (XSS and Planting of Malware) |
| 2 | Insufficient Anti-Automation (Brute Force and DoS) |
| 3 | Improper Input Handling (SQL Injection) |
| 4 | Insufficient Authentication (Stolen Credentials/Banking Trojans) |
| 5 | Application Misconfiguration (Detailed error messages) |
| 6 | Insufficient Process Validation (CSRF and DNS Hijacking) |
| 7 | Insufficient Authorization (Predictable Resource Location/Forceful Browsing) |
| 8 | Abuse of Functionality (CSRF/Click-Fraud) |
| 9 | Insufficient Password Recovery (Brute Force) |
| 10 | Improper Filesystem Permissions (info Leakages) |

| OWASP Top Ten 2010 | CWE/SANS Top 25 2010 |
|---|---|
| A1 - Injection | CWE-89 SQL injection, CWE-78 OS Command injection |
| A2 - Cross Site Scripting (XSS) | CWE-79 Cross-site scripting |
| A3 - Broken Authentication and Session Management | CWE-306 Missing Authentication for Critical Function, CWE-307 Improper Restriction of Excessive Authentication Attempts , CWE-798 Use of Hard-coded Credentials |
| A4 - Insecure Direct Object References | CWE-285 Improper Access Control (Authorization) |
| A5 - Cross Site Request Forgery (CSRF) | CWE-352 Cross-Site Request Forgery (CSRF) |
| A6 - Security Misconfiguration | No direct mappings; CWE-209 is frequently the result of misconfiguration. |
| A7 - Insecure Cryptographic Storage | CWE-327 Use of a Broken or Risky Cryptographic Algorithm, CWE-311 (Missing Encryption of Sensitive Data) |
| A8 - Failure to Restrict URL Access | CWE-285 Improper Access Control (Authorization) |
| A9 - Insufficient Transport Layer Protection | CWE-311 Missing Encryption of Sensitive Data |
| A10 - Unvalidated Redirects and Forwards | CWE-601 URL Redirection to Untrusted Site ('Open Redirect') |

| WASC Threat Classification v2 | OWASP Top Ten 2010 RC1 |
|---|--|
| WASC-19 SQL Injection | A1 - Injection |
| WASC-23 XML Injection | |
| WASC-28 Null Byte Injection | |
| WASC-29 LDAP Injection | |
| WASC-30 Mail Command Injection | |
| WASC-31 OS Commanding | |
| WASC-39 XPath Injection | |
| WASC-46 XQuery Injection | |
| WASC-08 Cross-Site Scripting | A2 –Cross Site Scripting (XSS) |
| WASC-01 Insufficient Authentication | A3 - Broken Authentication and Session |
| WASC-18 Credential/Session Prediction | |
| WASC-37 Session Fixation | |
| WASC-47 Insufficient Session Expiration | |
| WASC-01 Insufficient Authentication | A4 - Insecure Direct Object References |
| WASC-02 Insufficient Authorization | |
| WASC-33 Path Traversal | |
| WASC-09 Cross-site Request Forgery | A5 - Cross-Site Request Forgery |
| WASC-14 Server Misconfiguration | A6 - Security Misconfiguration |
| WASC-15 Application Misconfiguration | |
| WASC-02 Insufficient Authorization | A7 - Failure to Restrict URL Access |
| WASC-10 Denial of Service | |
| WASC-11 Brute Force | |
| WASC-21 Insufficient Anti-automation | |
| WASC-34 Predictable Resource Location | |
| WASC-38 URL Redirector Abuse | |
| WASC-50 Insufficient Data Protection | A9 - Insecure Cryptographic Storage |
| WASC-04 Insufficient Transport Layer Protection | |
| | A10 -Insufficient Transport Layer Protection |

Mapping von
Jeremiah Grossman
(+Bil Corry)

So long and thx for the fish

Fragen?

- Links:
 - ▶ [Top 10](#)
 - ▶ [Präsentation von Dave Wichers](#)