OWASP Top 10 – Wat nu?

OWASP Stamm-tisch

GUUG-Treffen

Dirk Wetter

Dr. Wetter IT-Consulting & -Services
mail bei drwetter punkt eu
dirk punkt wetter bei owasp punkt org
+49-(40)-2442035-1

C'est moi

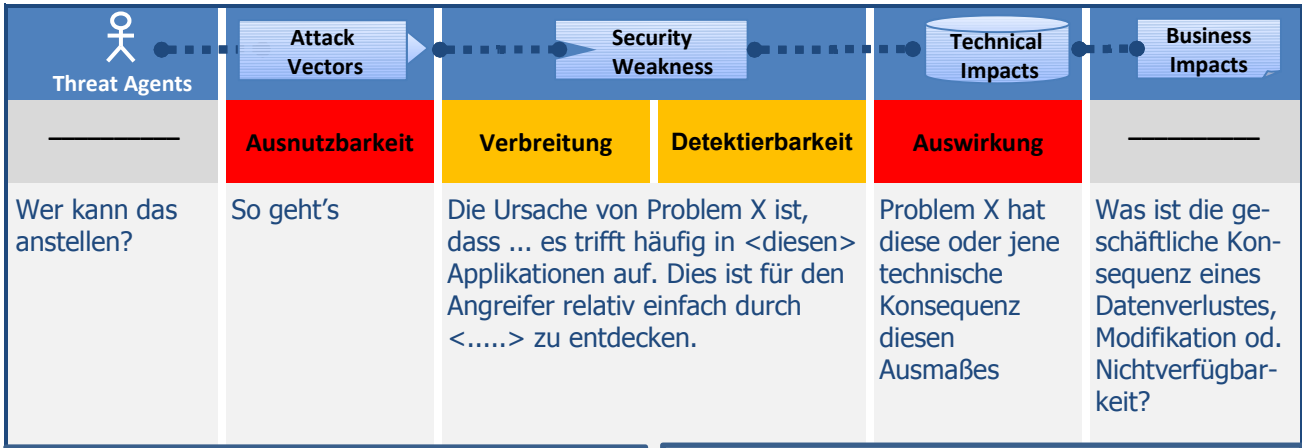
- Selbständig, IT-Sicherheitsberatung
- Engagiert in GUUG: Vorstand, Konferenzen
- Bisserl auch in OWASP
- Vom Herzen Unixer seit > 2 Dekaden
  - Netze!
  - (trotzdem kein Win-Dummy)
- Schreibe gerne

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

A# Problem X

Kausalkette
Bedrohung ... Auswirkung



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...

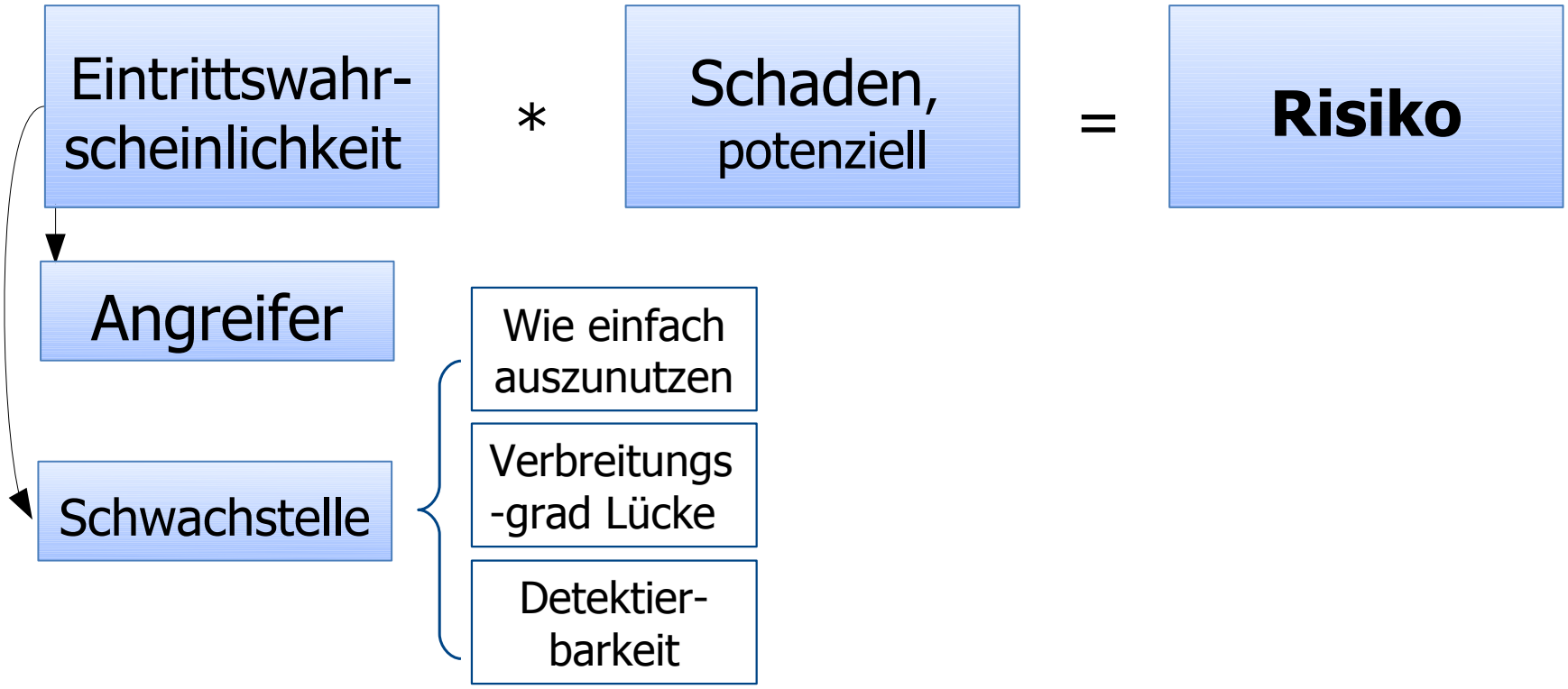
Schwachstellen vs. Risiken

- 2007 → **Schwachstellen**
  - webbezogene MITRE Vulnerability Trends aus 2006
- 2010 → **Risiken**
  - 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 Methology



It's all about Risk

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
_____	Ausnutzbarkeit	Verbreitung	Detektierbarkeit	Auswirkung	_____
Wer kann das anstellen?	So geht's	Die Ursache von Problem X ist, dass ... es trifft häufig in <diesen> Applikationen auf , Dies ist für den Angreifer relativ einfach durch <.....> zu entdecken.		Problem X hat diese oder jene technische Konsequenz diesen Ausmaßes	Was ist die geschäft-liche Konsequenz eines Datenverlustes, -Modifikation oder der Nichtverfügbarkeit?
Angreifer	Schwachstelle			technisch	monetär

Wie einfach auszunutzen

Verbreitungs -grad Lücke

Detektier-barkeit

Eintrittswahrscheinlichkeit

Schaden, potenziell

It's all about Risk

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
_____	Ausnutzbarkeit	Verbreitung	Detektierbarkeit	Auswirkung	_____
Wer kann das anstellen?	So geht's	Die Ursache von Problem X ist, dass ... es trifft häufig in <diesen> Applikationen auf , Dies ist für den Angreifer relativ einfach durch <.....> zu entdecken.		Problem X hat diese oder jene technische Konsequenz diesen Ausmaßes	Was ist die geschäft-liche Konsequenz eines Datenverlustes, -Modifikation oder der Nichtverfügbarkeit?
Angreifer	Schwachstelle			technisch	monetär

Wie einfach auszunutzen

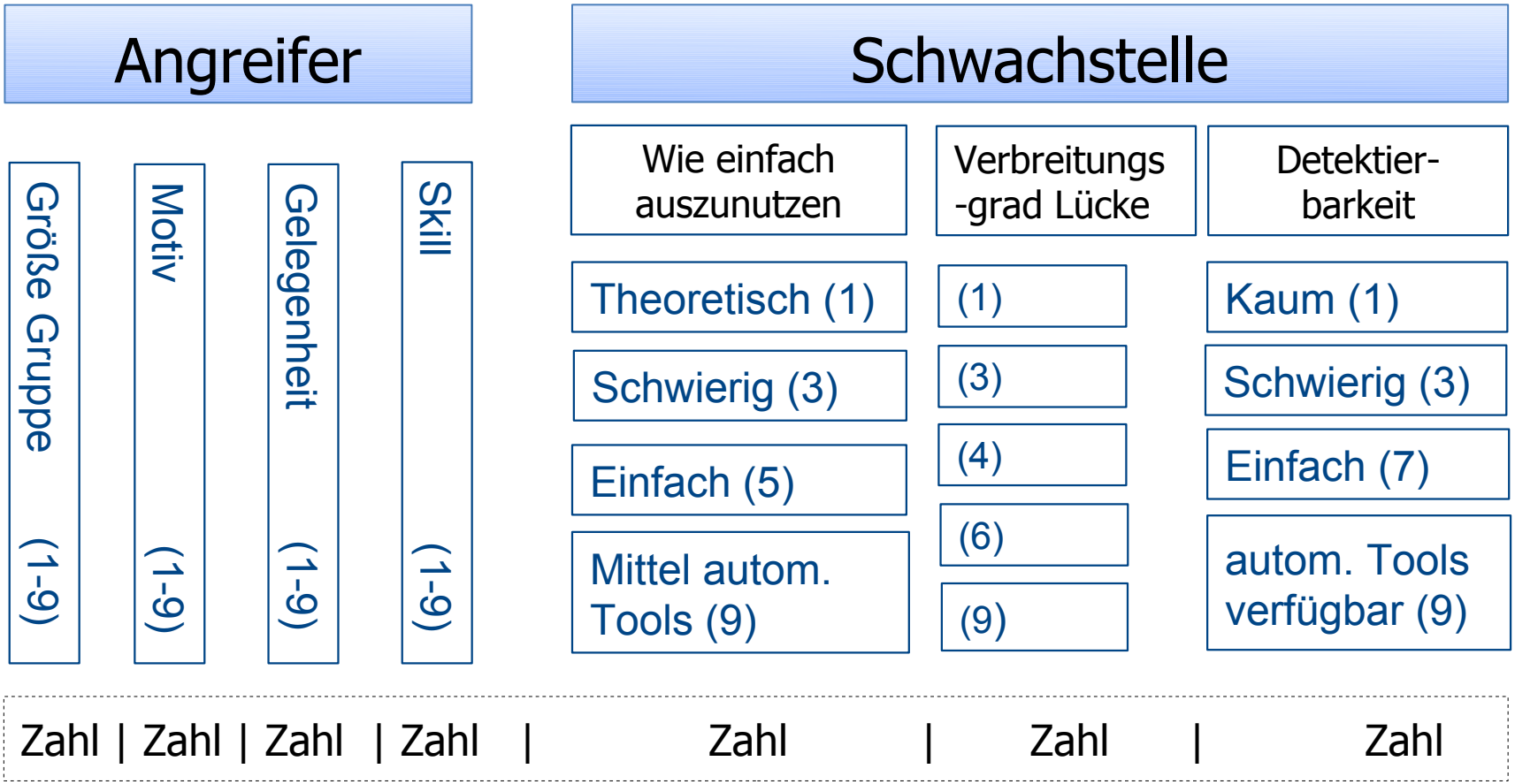
Verbreitungs -grad Lücke

Detektier-barkeit

Schaden, potenziell

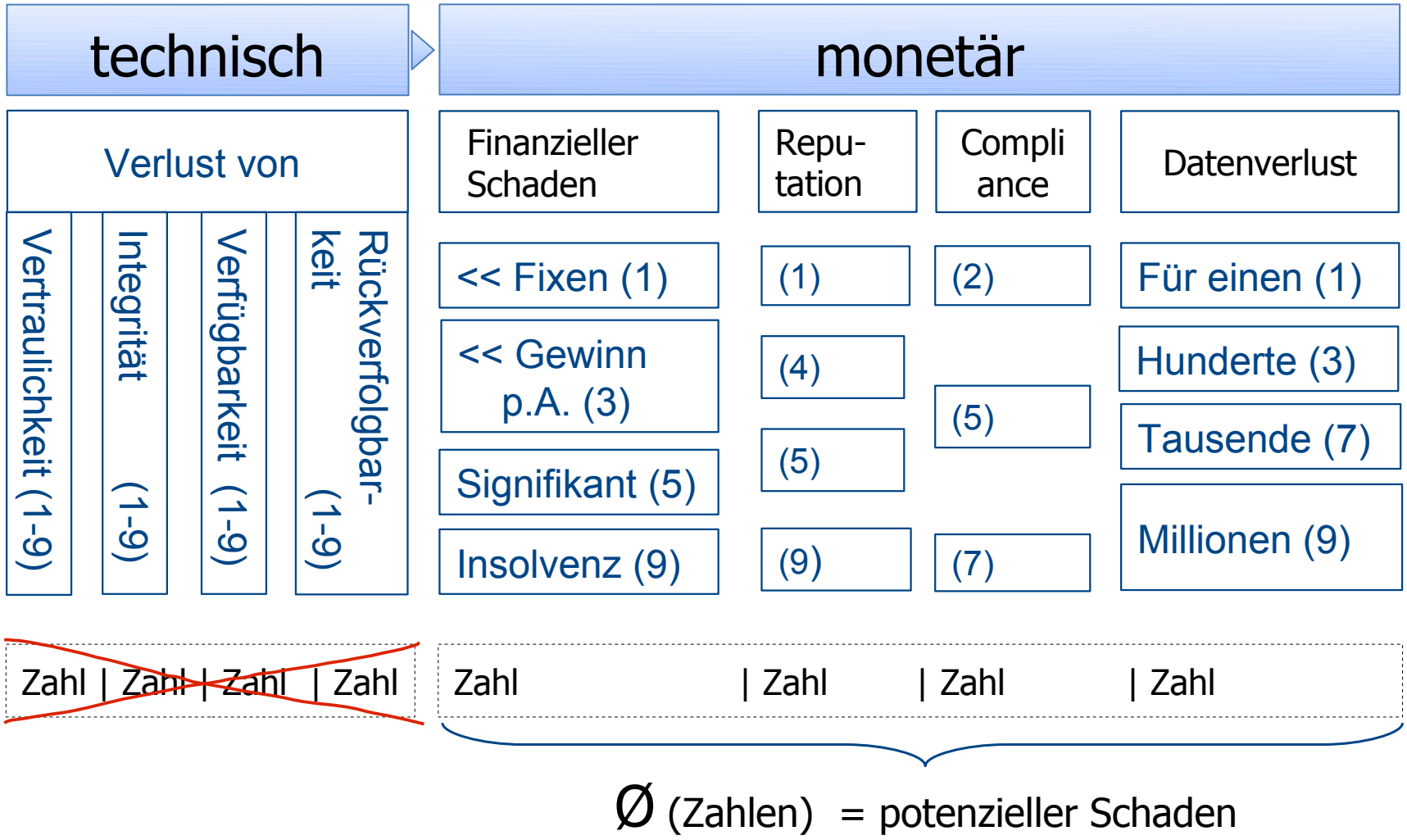
Eintrittswahrscheinlichkeit

Rate it!: Eintrittswahrscheinlichkeit

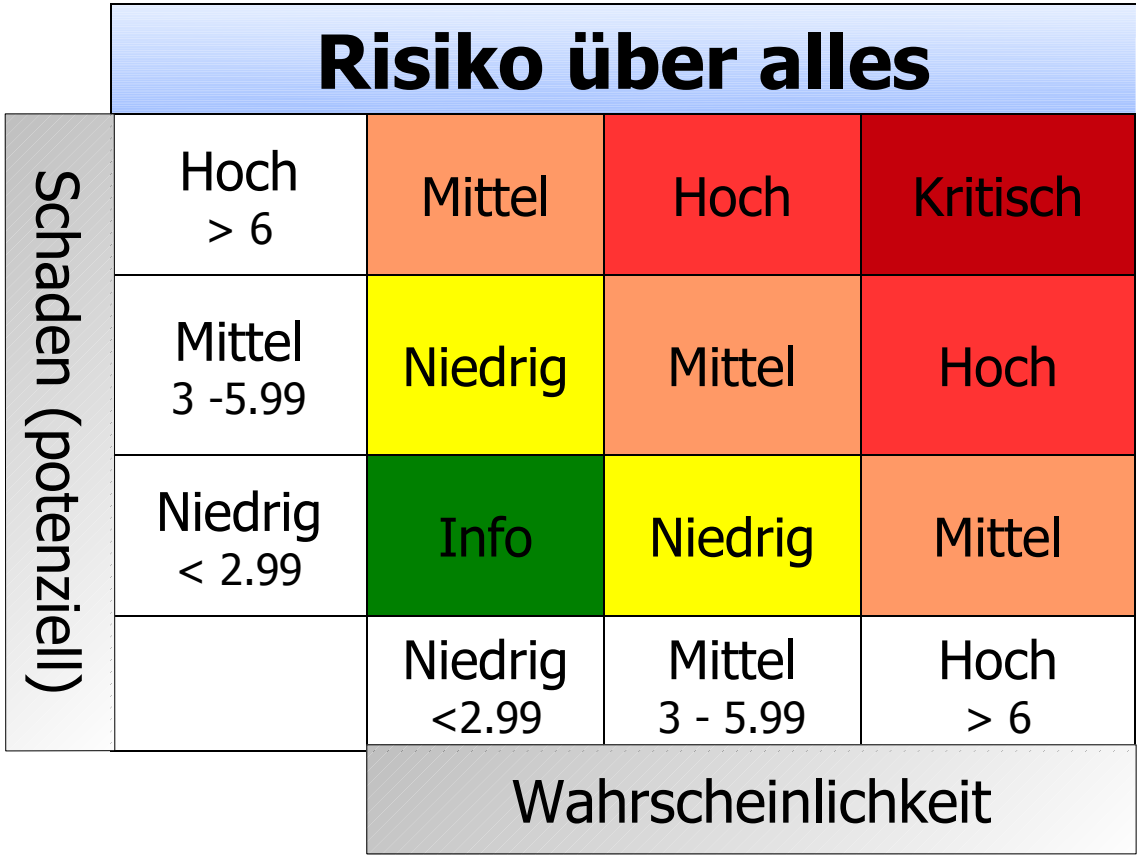


Ø (Zahlen) = Eintrittswahrscheinlichkeit

Rate it!: Schaden



Risikograph



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

Risiko: Wozu nun das Ganze?

- Risikomanagementprozess:
  - Erfassung
    - Analyse (Code / externer Audit)
    - Bewertung (s.o.)
  - Steuerung
  - Kontrolle

- Technisch: Strukturiert und priorisiert fixen
- Business: Rechte Balance zw. Geld und Sicherheit

- Mehr? Siehe ISO 27005, BSI 100-3 u.v.a.

	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 NEU!	~~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
A 10	Unvalidated Redirects and Forwards NEU!	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 NEU!	~~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
A 10	Unvalidated Redirects and Forwards NEU!	Failure to Restrict URL Access

Kritik

- **2007s A3 Malicious File Inlusion: RFI**
  - Laut zone-h (Q1 2010 Statistiken):
    - 2008 < 2009 < 2010
    - http://www.zone-h.org/news/id/4735

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

Kurz die Charts

A1. Injection Flaws

- Weiterreichen mangelhaft überprüfter Daten
- i.d.R.: Größter anzunehmender (technischer) Schaden
  - Datenzugriff, OS-Zugriff, ...

A2. XSS

- I/O mangelhaft überprüfter Daten
- Sehr verbreitet

16-jähriger demonstriert Sicherheitslücken bei 17 Banken

vorlesen / MP3-Download

Die nächste Ausgabe des c't magazins berichtet, dass der 16-jährige Schüler Armin Razmdjou auf den Web-Seiten von 17 Banken Sicherheitslücken entdeckt hat. Bei den Lücken handelt es sich um sogenannte Cross-Site-Scripting-Probleme, die eine besonders raffinierte Form des Phishings ermöglichen.

Sicherheitslücken bei Banken

Bilderstrecke, 17 Bilder

Er habe sich gewundert, dass heise Security bis vor etwa zwei Jahren intensiv über derartige Probleme berichtet hatte – mittlerweile aber so gut wie nichts mehr darüber zu lesen sei, erklärte der Zwölftklässler. Aus Neugier hat er selbst eine Reihe von Bankenseiten untersucht. In etwa 4 von 5 Fällen wurde er fündig und entdeckte eine Sicherheitslücke. heise Security konnte alle Probleme nachvollziehen und benachrichtigte die betroffenen Banken. Alle gemeldeten Lücken sind mittlerweile geschlossen.

Kurz die Charts

A1. Injection Flaws

- Weiterreichen mangelhaft überprüfter Daten
- i.d.R.: Größter anzunehmender Schaden
  - Datenbankzugriff, OS-Zugriff, ...

A2. XSS

- I/O mangelhaft überprüfter Daten
- Sehr verbreitet
- Schaden für Betreiberfirma i.d.R. begrenzter
  - Primäres Ziel: einzelner Account
  - Aber:
    - Stored XSS, Kombis mit CSRF: Würmer
    - Admin-Konto

Kurz die Charts

A3. Broken Authentication and Session Mgmt.

- Ziel: Account-Mgmt (PW/Session-ID)
  - Session-Fixation
  - Session-ID: Random?
  - PWs+Session-IDs über HTTPS? (gehört eher zu A9)
  - Erlauben schwacher PWs / kaputter Recovery-Funktionen
  - Oder: 4 stellige PINs und kein Limit für Lock
  - Laxe Timeouts
- Schaden u.U. Hoch

Apple's Worst Security Breach: 114,000 iPad Owners Exposed

Apple has suffered another embarrassment. A security breach has exposed iPad owners including dozens of CEOs, military officials, and top politicians. They—and every other buyer of the cellular-enabled tablet—could be vulnerable to spam marketing and malicious hacking.

It doesn't stop there. According to the data we were given by the web security group that exploited vulnerabilities on the AT&T network, we believe 114,000 user accounts have been compromised, although it's possible that confidential information about every iPad 3G owner in the U.S. has been exposed. We

Quelle: gawker.com 9.6.2010


```
89014104243219[redacted] : [redacted]@eucom.mil
89014104243220[redacted] : [redacted]@us.army.mil
89014104243220[redacted] : [redacted]@us.army.mil
89014104243220[redacted] : [redacted]@us.army.mil
89014104243220[redacted] : [redacted]@us.army.mil
89014104243315[redacted] : [redacted]@us.army.mil

89014104243221[redacted] : [redacted]@nasa.gov
89014104243221[redacted] : [redacted]@nasa.gov
89014104243221[redacted] : [redacted]@faa.gov
89014104243221[redacted] : [redacted]@faa.gov
89014104243221[redacted] : [redacted]@usdoj.gov
89014104243315[redacted] : [redacted]@fcc.gov
89014104243315[redacted] : [redacted]@mail.house.gov
89014104243221[redacted] : [redacted]@fjc.gov
```

In the media and entertainment industries, affected accounts belonged to top executives at the New York Times Company, Dow Jones, Condé Nast, Viacom, Time Warner, News Corporation, HBO and Hearst.

```
89014104243220[redacted] : [redacted]@nytimes.com      <-- Janet Robinson, CEO of NY Times
89014104243219[redacted] : [redacted]@time.com         <-- Ann Moore, CEO of Time Inc.
89014104243221[redacted] : [redacted]@newscorp.com     <-- Chase Carey, President/COO of News Corp.
89014104243315[redacted] : [redacted]@hearst.com       <-- Cathie Black, President of Hearst Magazines
89014104243315[redacted] : [redacted]@dowjones.com     <-- Les Hinton, CEO of Dow Jones
89014104243221[redacted] : [redacted]@weinsteinco.com  <-- Harvey Weinstein, Co-Founder of Weinstein Co.
89014104243315[redacted] : [redacted]@bloomberg.net    <-- Michael Bloomberg, Founder of Bloomberg LP
```

Within the tech industry, accounts were compromised at Google, Amazon, Microsoft and AOL, among others. In finance, accounts belonged to companies from Goldman Sachs to JP Morgan to Citigroup to Morgan Stanley, along with dozens of venture capital and private equity firms.

In government, affected accounts included a GMail user who appears to be Rahm Emanuel and staffers in the Senate, House of Representatives, Department of Justice, NASA, Department of Homeland Security, FAA, FCC, and National Institute of Health, among others. Dozens of employees of the federal court system also appeared on the list.

Quelle: gawker.com 9.6.2010

Kurz die Charts

A4. Insecure Direct Object References

- An **T-Hack** denken
  - POST/GET-Parameter bestimmt Konto
- Oder Path Traversal / LFI
- Schaden laut Top 10 moderat (m.E. potenziell hoch)

A5. Cross-Site Request Forgery

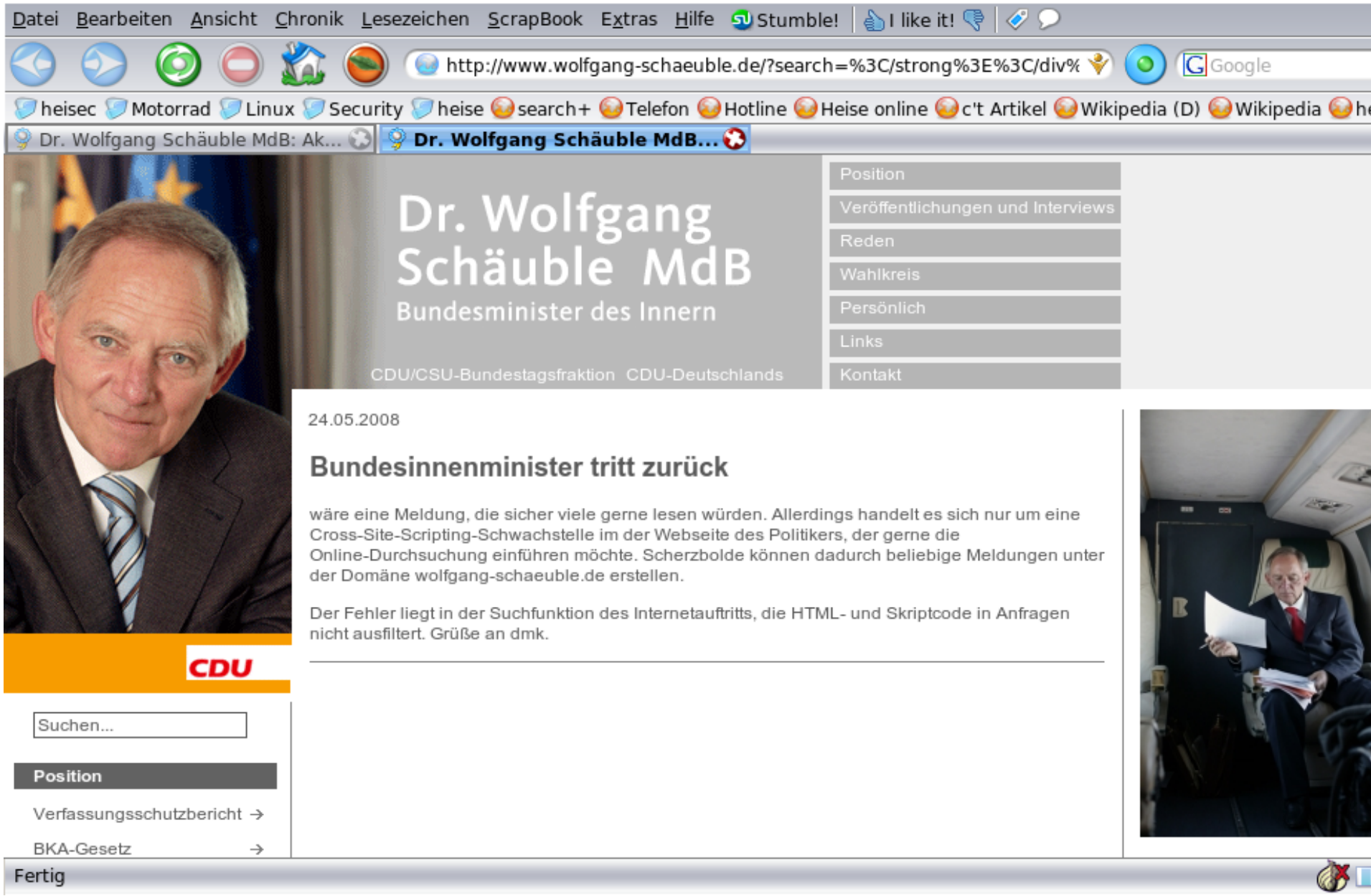
- Statuslosigkeit HTTP, Browser wird Request untergeschoben
- Transaktionen ohne (weitere) User-Aktionen
- Schaden (allein): moderat
  - Abseits Massenrequests (DNS-pharming DSL-Router .mx)

Kurz die Charts

A6. Security Misconfiguration

- Eher ein Infrastrukturthema
  - ungepatcht
  - fehlkonfiguriert
  - Default-Reste

  } in DB, OS, PWs, App?
- Betrifft besonders Patches für App-Framework!!
  - heikles Thema gerade bei SW Dritter
- Schaden: moderat



Bildquelle: heise security 28.05.2008

Kurz die Charts

A7. Insecure Cryptographic Storage

- Alles (hinreichend gut) verschlüsselt, was verschlüsselt gehört?
  - DB-Dumps/Backups
  - Logins/PW?
  - Vorsicht: Insider
- Schlüssel-Handling ok?
- Schaden groß:

  Datengau

Kurz die Charts

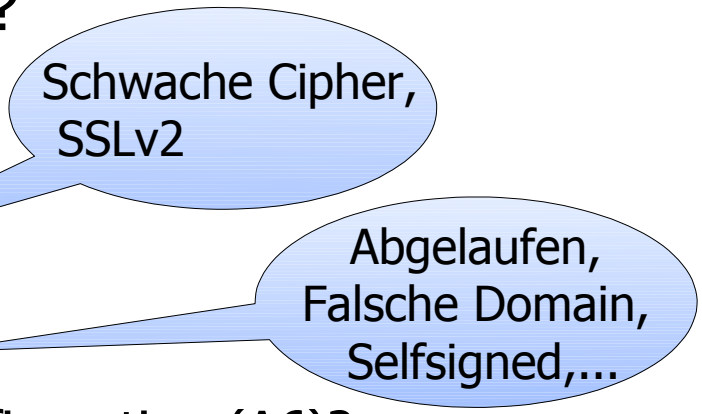
A8. Failure to Restrict URL Access

- Access-Control-Problem
  - Bypass von Authentifizierung
  - Oder keine genügende
- Schaden moderat

Kurz die Charts

A9. Insufficient Transport Layer Protection

- SSL/TLS überall wo nötig?
- Cookie: Secure-Flag?
- Lt. OWASP auch
  - SSL-Konfigurations-
  - und Zertifikatsprobleme
  - Nicht eher Security Misconfiguration (A6)?



Kurz die Charts

A10. Unvalidated Redirects and Forwards

- Mangelnde Eingabe-Validierung
- Kann Angreifer Redirect-Ziel vorgeben?
  - Frage gefallen lassen: Warum überhaupt parametrisierte R+F?
- Schaden: Moderat
  - Eher Phisher, die einzelne/mehrere Accounts kompromittieren

Blick über den OWASP-Tellerrand

- **SANS/CWE**

  Common Weakness Enumeration
  A Community-Developed Dictionary of Software Weakness Types

  Top 25 Most Dangerous Software Errors

  - Weaknesses!
  - Wie bei OWASP T10 2007

    lieferte MITRE das Ranking
    - Gut strukturiert
      - Top 25 eine Seite (ok...)
      - Mit Verweis auf jeweiligen CWE (http://cwe.mitre.org/data/definitions/<zahl>.html
    - Ausführlicher!
  - Verschiedene Ziele

Blick über den OWASP-Tellerrand

- **SANS/CWE**

  Top 25 Most Dangerous Software Errors

- Interessant:
  - Software Error Categories:
    - Insecure Interaction Between Components (8 errors)
    - Risky Resource Management (10 errors)
    - Porous Defenses (7 errors)

- 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
  - http://projects.webappsec.org/f/WASC-TC-v2_0.pdf
  - 172 Seiten (!)
  - 49 Punkte
  - Views
    - Threat Classification Enumeration View
    - Development Phase View
    - Taxonomy Cross Reference View
      (hier super mapping WASC vs. SANS/CWE vs. OWASP 2010 u.a.)

Blick über den OWASP-Tellerrand

- **WASC Threat Classification v2.0**

- "Threats" auf den Punkt gebracht
- Halt lang
- Akademische Ausarbeitung
- Gute Erklärung der "Threats"
  - Code
  - Stellenweise Überschneidungen
- Risiko und Vermeidung?

Blick über den OWASP-Tellerrand

- **WHID Top 10 Risks for 2010**
  - DB: http://www.xiom.com/whid/
  - https://wasc-whid.dabbledb.com/page/wasc-whid/dXhcaN
    - Auch ein WASC-Projekt
    - Sicherlich nicht komplett
  - Fokus eher Incidents
    - Und nur ausgesuchte
    - Real world
  - http://projects.webappsec.org/w/page/Web-Hacking-Incid
  - 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	A8 - Unvalidated Redirects and Forwards
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?

- Mehr
  - Top 10
  - Präsentation von Dave Wichers