Hamburg @work

Arbeitskreis Security

SE | 07 SOFTWARE ENGINEERING

Softwaretechnik und Sicherheit. - ein Widerspruch?

Peter J. Wirnsperger
Enterprise Risk Services – Deloitte.
Leiter des Arbeitskreis Security von Hamburg@Work

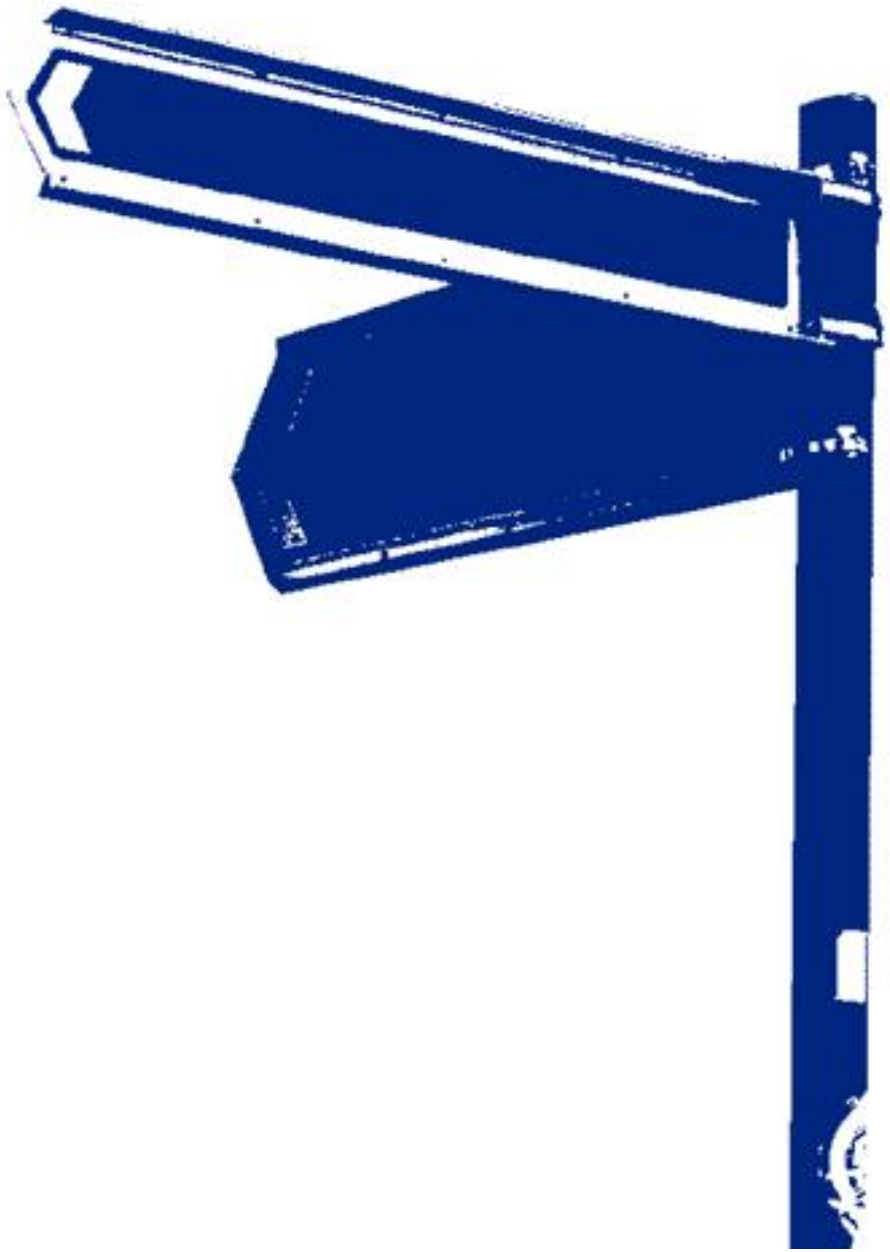
28. März 2007

Deloitte.
Wirtschaftsprüfung . Steuerberatung . Consulting . Corporate Finance .

Agenda

- Eine unvollständige Bestandsaufnahme
- Das Umfeld
- Wo liegt das Problem?
- Diskussion

Eine unvollständige Bestandsaufnahme



Bestandsaufnahme
Inhaltsanalyse

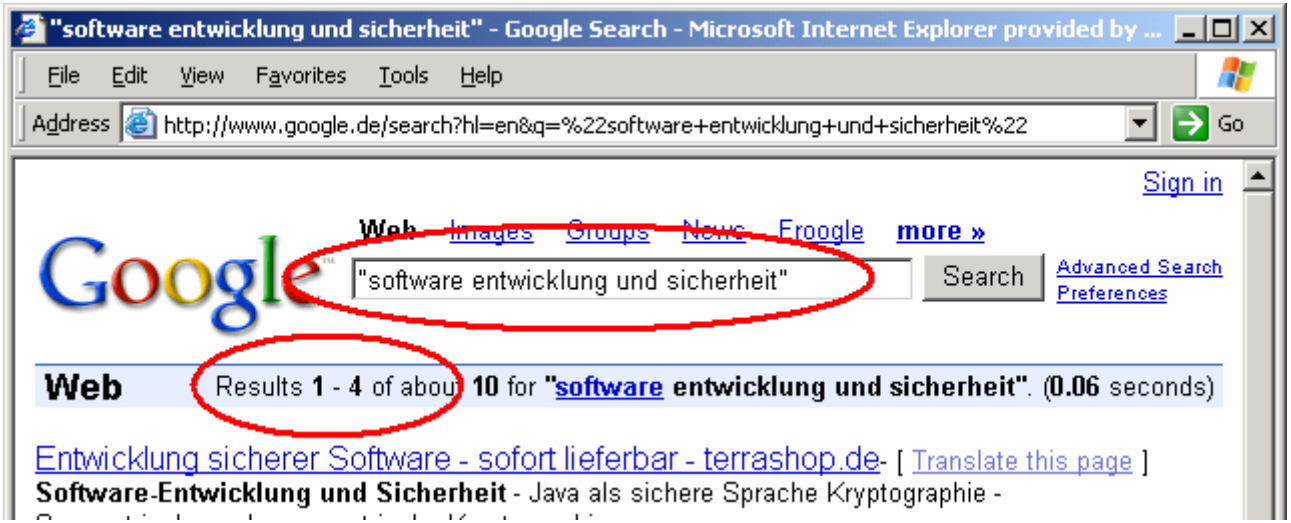
- Kongressprogramm SE 2007

  55 Vorträge -> 2 Vorträge mit dem Begriff „Security“ im Titel

- Google

  Suche: „Software-Entwicklung und Security“

  Ergebnis: 4 Einträge!!!



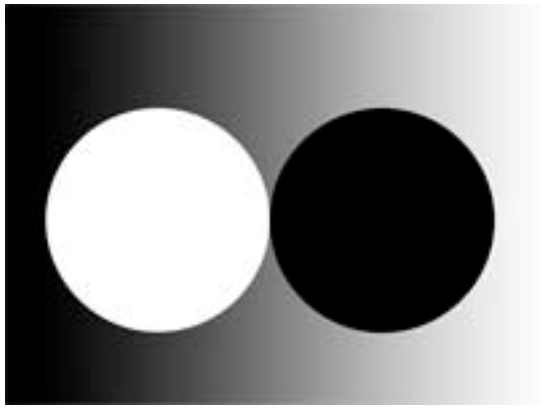
Bestandsaufnahme
Tatsachen: OWASP TOP 10

	Die 10 kritischsten Verwundbarkeiten in Web Applikationen (2007):	
✓	A1	Cross Site Scripting (XSS)
✓	A2	Injection Flaws
	A3	Insecure Remote File Include
	A4	Insecure Direct Object Reference
	A5	Cross Site Request Forgery (CSRF)
✓	A6	Information Leakage and Improper Error Handling
✓	A7	Broken Authentication and Session Management
	A8	Insecure Cryptographic Storage
✓	A9	Insecure Communications
✓	A10	Failure to Restrict URL Access
	Quelle: OWASP Foundation	

Bestandsaufnahme
Software-Entwicklung und Security

Gegensätze oder Wertepaare?

- Feuer & Eis
- Sonne & Mond
- Schwarz & Weiß



oder

- Ying & Yang

Bestandsaufnahme
Anforderung an Software

Verlässliche Software macht,
was sie machen soll.

Sichere Software macht,
was sie machen soll … und **NICHTS** anderes!

Umfeld
Erweiterte Funktionalität und steigende Komplexität

Steigende Komplexität der Anwendungslandschaft:

- **Unternehmen**: Kundenservice & administrative Funktionen
- **Externe Provider**: Front-End-Web-Farmen und Anwendungshosting
- **Partner Schnittstellen**: Datenströme (Lagerhaltung, Zahlung, Real-Time-Verarbeitung)

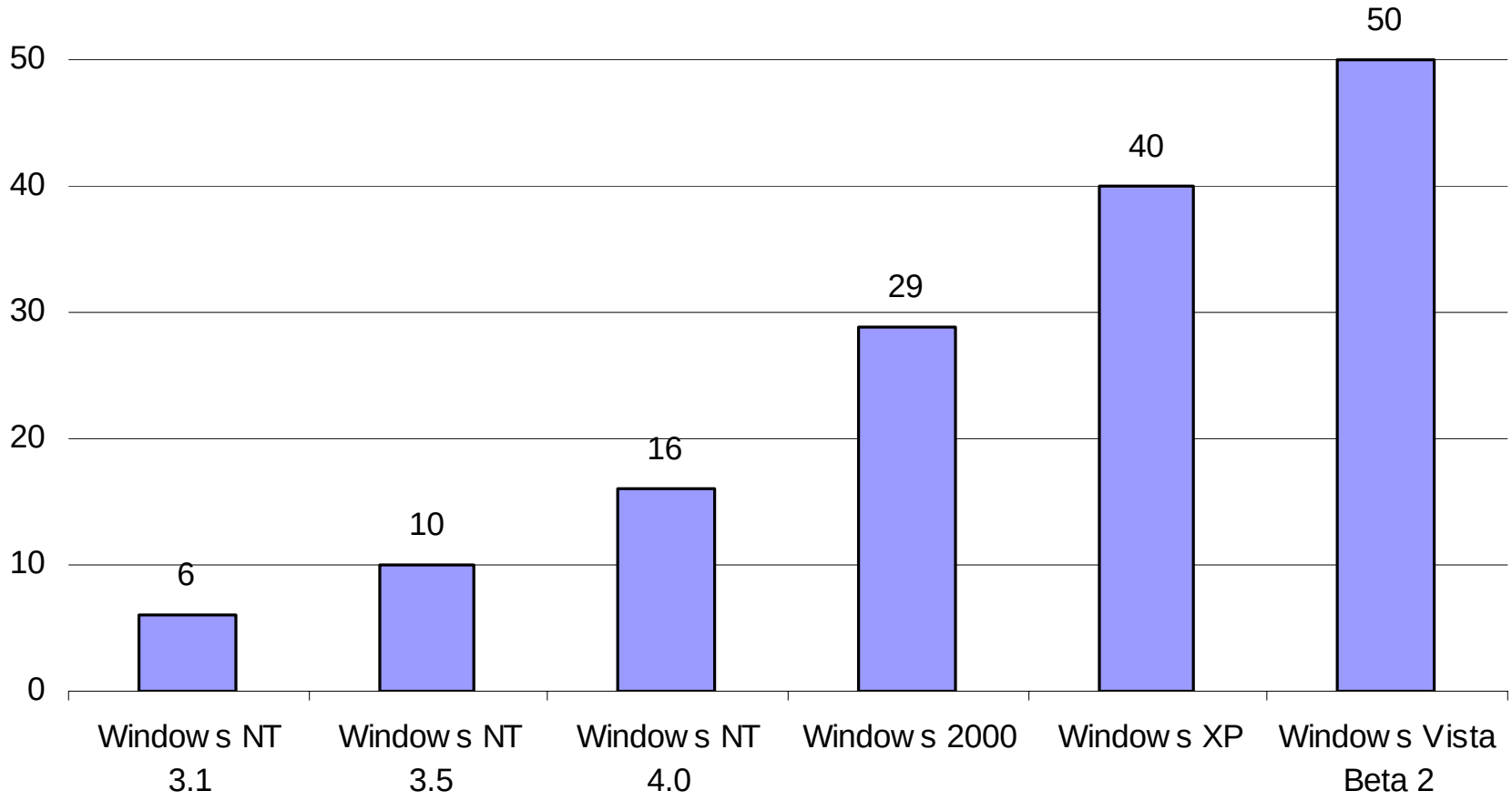
- Anwendungslandschaften werden komplexer
  - Mainframe → Client-Server → *n*-tier → SOA (J2EE und .Net)

- Netzwerk Service Verlagerung
  - Bandbreite, Hosting, Provisioning, Service-Erbringung

⇨ Anwendungen verknüpfen mehrere Bereiche über alle Schichten hinweg.

Umfeld
Mengenwachstum der SLOC

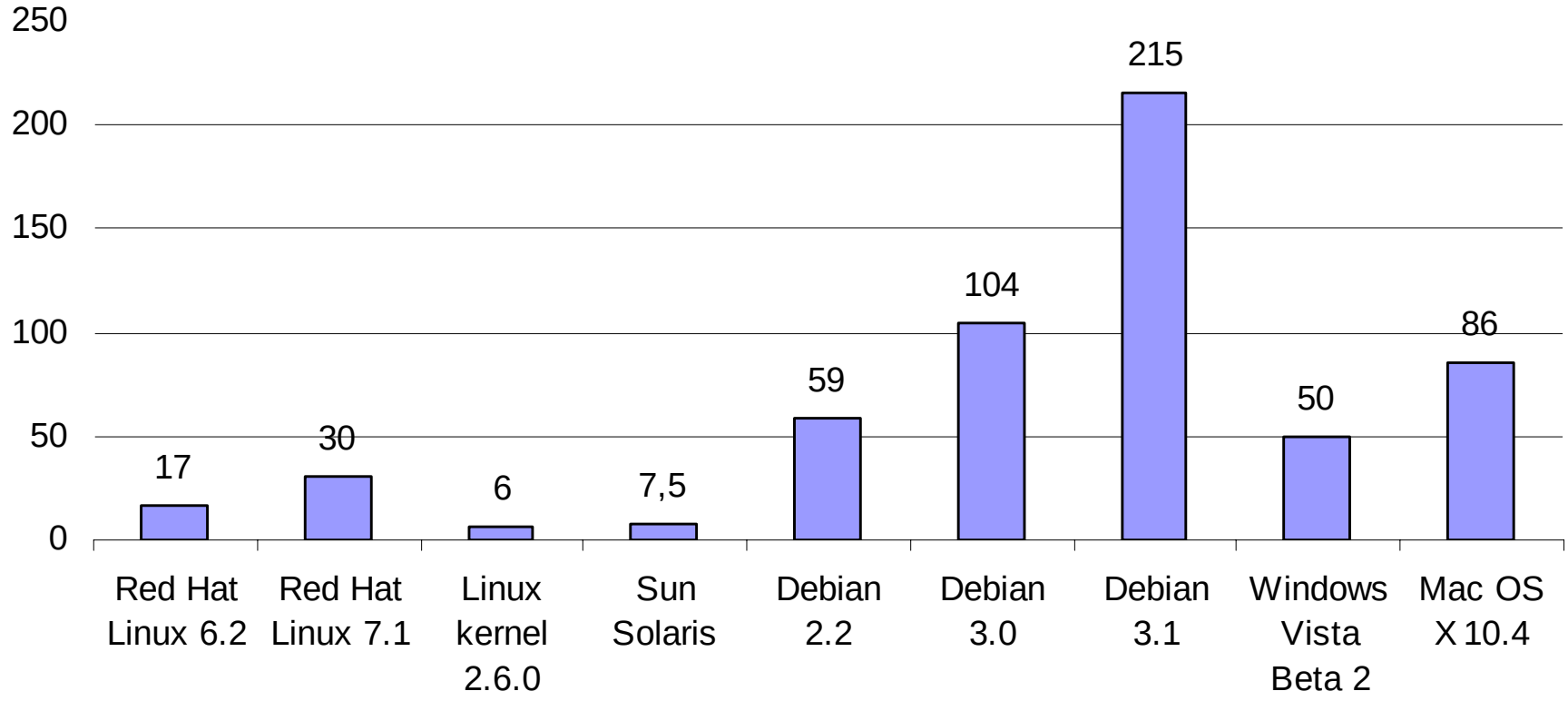
Entwicklung der „Source Lines of Code“ (SLOC) bei Windows in Mio.



Quelle: Wikipedia 21.3.2007

Umfeld
Mengengerüst SLOC in Betriebssystemen

SLOC bei ausgewählten Betriebssystemen in Mio.



Quelle: Wikipedia 21.3.2007

Wo liegt das Problem?

Wo liegt das Problem
Steigende Komplexität

Wer hat den Überblick?

„The Central Enemy of Reliability is Complexity.
Complexity is the Enemy of Security“
Dan Geer

Wo liegt das Problem
unvollständige Denkmodelle?

Alle Wege führen nach Rom!

Welcher Weg ist sicher?

- ⇨ Beinhaltet die Aufgabenstellung die Frage nach Sicherheit oder ist Sicherheit das Problem der anderen?
- ⇨ Wer hat den Mut im Projekt die Frage nach Sicherheitsfunktionen zu stellen? ;-)
- ⇨ Ist im Projekt Platz (Budget, Zeit, Verständnis) für die Lösung der Sicherheitsfrage?

Wo liegt das Problem
Ein Lösungsansatz?

Sicherheit ist ein Teil der Qualität

Qualität beinhaltet aber nicht zwingend Sicherheit

Sicherheit ist eine eigenständige Funktion

Diskussion

Diskussion
Pointierte Aussagen

- Normen und Rahmenwerke für Software-Entwicklung verfolgen in erster Linie den Qualitätsgedanken.

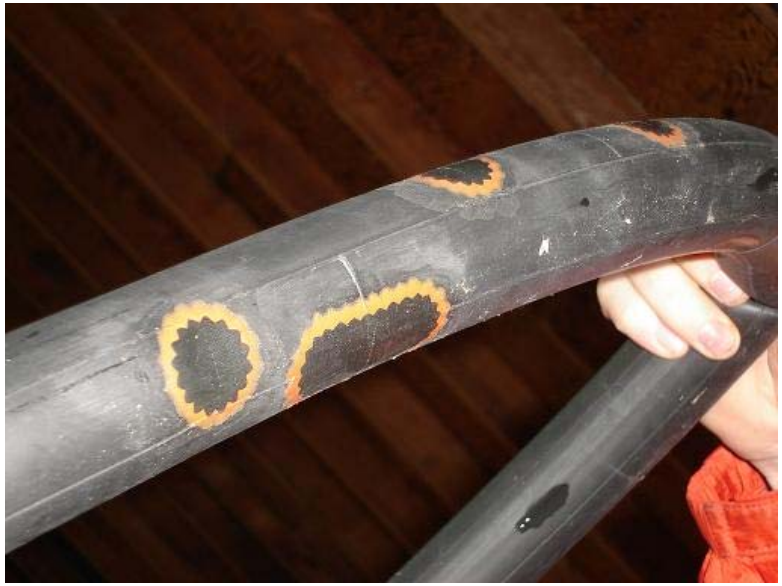
- Software-Entwicklung zielt im Normalfall nicht explizit auf Sicherheit.
  ⇨ Ausrichtung auf die Lösung

- Implizite Sicherheitsmechanismen bestimmen das Maß an Sicherheit.
  ⇨ Trust-Model

- Open-Source ist sicher – Closed Source ist unsicher
  ⇨ Was sagt die Statistik?

Diskussion

- Wie kommt die Sicherheit von Anfang an in die Software?
- Was muss sich ändern, damit Software sicher entwickelt und ausgeliefert wird?



Deloitte.

Kontakt Information

Deloitte.

Peter J. Wirnsperger

Senior Manager
Enterprise Risk Services

Axel-Springer-Platz 3
20355 Hamburg
Tel.: + 49 40 32080 4675
Fax: + 49 40 32080 4702
Mobile + 49 172 3690 675
email: pwirnsperger@deloitte.de
www.deloitte.com/de/security