



Das secologic Projekt im Kurzüberblick - Stand Sept. 2005 -

EUROSEC GmbH Chiffriertechnik & Sicherheit

Autor: Dr. Thilo Zieschang, EUROSEC

Tel: 06173 / 60850, www.eurosec.com

© EUROSEC GmbH Chiffriertechnik & Sicherheit, 2005

secologic Projekt

- Projektgegenstand: Methoden und Werkzeuge zur Entwicklung Sicherer Software
- Konsortialpartner:
 - SAP
 - Commerzbank
 - Universität Hamburg
 - EUROSEC
- Laufzeit: 2005 und 2006
- Gefördert vom Bundesministerium für Wirtschaft

Problembeschreibung

- Die überwiegende Mehrzahl auftretender IT-Sicherheitsprobleme beruht auf zwei Grundproblemen: fehlerhafte Konfiguration einerseits, und fehlerhafte Programmierung andererseits.
- Bisherige, in Forschungseinrichtungen entwickelte Methodiken und Lösungsansätze zur Vermeidung von Sicherheitsproblemen in der Softwareentwicklung konnten sich in der Praxis nicht ausreichend durchsetzen.

Fehlende Lösungen und dringender Handlungsbedarf

- Wenngleich es mittlerweile hochentwickelte, ausgezeichnete Software Engineering Methoden und CASE Tools gibt, auch zur Unterstützung bzw. Lösung von Sicherheitsfragen, entsprechen deren Zielsetzung und typisches Anwendungsprofil nicht immer den Praxisanforderungen.

==> Hieraus ergibt sich aktueller Handlungsbedarf, zur Wahrung der Interessen der betroffenen Softwarehersteller sowie ihrer Kunden und Anwender.

==> Erarbeitung, Erprobung und Nutzbarmachung von Methoden und Werkzeugen, die den Praxis-Anforderungen entsprechen, sind Ziel des secologic Projekts.

Art der angestrebten Resultate

- Best Practice Beschreibungen
- Fachartikel und technische Analysen
- Checklisten zur Überprüfung durch Reviewer
- Software-Komponenten z.B. für Input Validation
- Schulungskonzepte und -unterlagen
- Web Tools (Questionnaires) zur Selbst-Evaluation
- exemplarisch nach den entworfenen Regeln erstellte Anwendungssoftware
- Case Studies mittels Sicherheitsanalyse vorhandener Software, inklusive Code Reviews

Arbeitspakete (Auswahl)

- Anforderungen an Skriptsprachen und PlugIns in Web-Applikationen
- Design- und Architektur-Empfehlungen für die Planung neuer Anwendungsprogramme
- Erstellung generischer Input Validation Prozeduren (Software Tools)
- Buffer Overflow Detection / Prevention
- Formulierung einer Methodik zum Application Security Testing
- Erarbeitung eines Schulungsplans für Softwareentwickler
- Gezielte Öffentlichkeitsarbeit

Publikation & Nutzen für die Öffentlichkeit

- angemessene Sicherheit ist immer auch Wettbewerbsvorteil und Marketingargument
- daher sollen möglichst viele Resultate publiziert werden
- geplant sind: Publikationen, Schulungen, Kongresse, Software Tools, u.v.m.
- Flankierung entsprechender BSI-Aktivitäten: Grundsatzhandbuch-Baustein „Systementwicklung“, ergänzt durch unsere Richtlinien-Dokumente

3	4	5	6	7	8
0	0	0	0	0	0
3	4	5	6	7	8
		1			
		2			
2	3	3	3	3	3
		4			
		5			
3	4	5	6	7	8
6	6	6	6	6	6
		7			
		8			
9	9	9	9	9	9
3	4	5	6	7	8
0	0	0	0	0	0
3	4	5	6	7	8
		1			
		2			
2	3	3	3	3	3
		4			
		5			
3	4	5	6	7	8
6	6	6	6	6	6
		7			
		8			

Aktueller Stand des secologic Projektes (Gesamtsicht)

Aktuelle Arbeiten und Ergebnisse (Stand Sept. 2005)

- „Sicher Programmieren in Java“ (Status: Reviewvorlage)
- „Java Script und Cross-Site Scripting“ (Status: Reviewvorlage)
- „Sicher Programmieren in C/C++“ (Status: Reviewvorlage)
- „Session Management in Webapplikationen“ (Status: in Arbeit)
- „Befragung (Status- und Bedarfsanalyse)“ (Status: in Arbeit)
- interner Webbereich für Konsortialpartner (Status: fertig)
- „Projektwebseite www.secologic.org“ (Status: fertig)
- „Erstellung von Testleitfäden“
- „Vorbereitung secologic Kongress“ (Status: in Arbeit)
- „Vorbereitung 1.Tagung des offenen Arbeitskreises“ (Status: in Arbeit)
- Mitarbeit BSI Grundschutztag (2 Vorträge der EUROSEC) (Status: fertig)

Nächste Termine und Treffen

- BSI Grundschutztag mit Vorstellung des Bausteins Sichere Systementwicklung, 21.09.05
- 1.secologic Arbeitskreis für interessierte Unternehmen, Oktober 2005, Steigenberger Hotel, Frankfurt
- 1.secologic InfoDay, 22. November 2005, Steigenberger Hotel, Frankfurt
- Fachseminar „Sichere Anwendungsentwicklung“, 23. November 2005, Steigenberger Hotel, Frankfurt
- Weitere Arbeitskreis-Meetings?