OWASP
Secure Software Contract Annex
- auf Deutsch -

German OWASP Day 2015
Lightning Talk, 01.12.2015, 14:50 - 15:00
Ralf Reinhardt, sic[!]sec GmbH

Gewerkschaftshaus
Wilhelm-Leuschner-Straße 69, 60329 Frankfurt am Main

*“Robust gegen Cross-Site Scripting?!
Das stand so nie im Fachkonzept!!”*

Aussage eines Lieferanten,
der einen kostenfreien Fix im Rahmen
der Gewährleistung strikt ablehnte.

München, etwa im Jahr 2008

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

“This contract Annex is intended to help software developers and their clients negotiate and capture important contractual terms and conditions related to the security of the software to be developed or delivered.”

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex_German

Ein USA-zentrisches “legal topic” - auf Deutsch?
IT meets Jura, von der Idee zur Zusammenarbeit:

Thomas Hofer, Akademischer Direktor

LMU München, Rechtsinformatikzentrum
Prof.-Huber-Platz 2
80539 München

www.jura.uni-muenchen.de/fakultaet/riz

Ralf Reinhardt

sic[!]sec GmbH
Industriestr. 29-31
82194 Gröbenzell

www.sicsec.de

Operative Umsetzung, Übersetzung

- Mareike Zeisel, Jahrgang 1990
- Seit 10/2015 im Rechtsreferendariat
- Nebentätigkeit “Vertragsmanagement” in einem Münchner Softwareunternehmen
- Soziales Engagement im Refugee Law Clinic Munich e.V., IT- und Rechtsfragen
- Nach Referendariat: Tätigkeitsschwer-punkt IT-Recht / Datenschutzrecht

Ergänzende Vertragsbedingungen zur Entwicklung von sicherer Software

“Warnung: Dieses Dokument ist ausschließlich als Orientierungshilfe anzusehen.

OWASP empfiehlt Ihnen inständig einen **spezialisierten Rechtsanwalt** zur Ausarbeitung eines Software-lizenzvertrages heranzuziehen.”

2. Philosophie

“(e) Sicherheitsinformationen werden vollständig offengelegt

[…]

Alle sicherheitsrelevanten Informationen werden zwischen dem Kunden und dem Entwickler unmittelbar und vollständig freigegeben.”

3. Maßnahmen zur Lebensdauer

“(d) Umsetzung
Jeglicher sicherheitsrelevanter Code muss gründlich kommentiert werden. **Spezifische Leitlinien** […] sollen darin enthalten sein. […] der gesamte **Code** von mindestens einem **anderen Entwickler** […] **überprüft**, bevor er als bereit für den Unit-Test erachtet wird.”

4. Themenbereich Sicherheitsanforderungen

“(a) Eingabeüberprüfung und Encoding
(b) Authentifizierung und Session Management
(c) Zugangskontrolle
(d) Fehlerbehandlung
(e) Protokollierung
(f) Anbindungen an externe Systeme
(g) Verschlüsselung
(h) Verfügbarkeit
(I) Sichere Konfigurierung
(j) Besondere Schwachstellen”

8. Sicherheitsüberprüfung

“**(a) Recht auf Überprüfung**

Kunde hat das Recht, die Software jederzeit innerhalb von 60 Tagen ab Lieferung auf Sicherheitslücken überprüfen zu lassen. Entwickler verpflichtet sich [...] durch die Bereitstellung von Quellcode und den Zugang zu Testumgebungen zu unterstützen.

(b) Prüfbericht

Sicherheitsüberprüfungen werden alle Aspekte der gelieferten Software abdecken, einschließlich benutzerdefinierter Codes, Komponenten, Produkte und Systemkonfiguration.”

Ausblick SoSe 2016 oder WiSe 2016/17

Aktueller Stand:
Es liegt eine **reine Übersetzung** vor.

Geplant für die nächste Studienarbeit, bzw. Workshop am Rechtsinformatikzentrum:
Juristische Würdigung und falls erforderlich **Anpassung an deutsche Rechtsnormen.**

Kontaktmöglichkeiten und weiter Informationen

http://www.owasp.de/

https://www.owasp.org/

https://lists.owasp.org/mailman/listinfo/owasp-germany (join us!)

Ralf Reinhardt

ralf.reinhardt@owasp.org
ralf.reinhardt@sicsec.de