Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

VUSC – DER CODESCANNER

SOFTWARE SCANNEN, SCHWACHSTELLEN FINDEN

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Steven Arzt
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-336
Fax 06151 869-224
steven.arzt@sit.fraunhofer.de
www.sit.fraunhofer.de

Software sollte Mindestanforderungen an IT-Sicherheit erfüllen. Doch wie erkennt man, ob eine frische App, ein ergänzendes Software-Update oder ein Stück Code sicher ist? VUSC, der Codescanner des Fraunhofer-Instituts für Sichere Informationstechnologie SIT, prüft Software automatisiert und detektiert Schwachstellen innerhalb von Minuten. Im Gegensatz zu anderen Softwarescannern benötigt VUSC keinen Quellcode. Weiterer Pluspunkt: VUSC arbeitet on premises und nicht in der Cloud – dadurch haben Nutzer jederzeit volle Kontrolle über ihre Daten.

Ist die Software, die für das eigene Unternehmen gekauft werden soll, auch sicher? Ist die Arbeit des externen Softwareentwicklers fehlerfrei? Ist die selbst entwickelte App wirklich sicher? Mithilfe von VUSC lassen sich diese Fragen schnell beantworten. Per drag and drop wird die zu untersuchende Datei einfach in den Scanner geladen, und ein paar Minuten später zeigt VUSC das Ergebnis der Sicherheitsprüfung an. Dafür braucht der Fraunhofer-Scanner weder den Quellcode, noch muss die zu prüfende Software zu fremden Servern geschickt werden.

Schwachstellen finden und bewerten

VUSC findet nicht nur Sicherheitslücken, sondern gibt zu jeder Schwachstelle eine allgemein verständliche Beschreibung des Problems. Darüber hinaus erstellt VUSC automatisch eine Klassifizierung der Schwachstellen. So sehen Nutzer auf einen Blick, ob die gefundene Schwachstelle ein hohes, mittleres oder geringes Risiko darstellt. Mithilfe dieser übersichtlichen Priorisierung können sie zuerst die schwerwiegendsten Fehler beheben.

Darüber hinaus liefert VUSC zahlreiche Detailinformationen zu den gefundenen Sicherheitslücken: Welche Daten sind betroffen? Wohin werden sie gesendet? Welche Art der Verschlüsselung nutzt die geprüfte Software? VUSC-Nutzer erhalten so eine Übersicht über konkrete Risikofaktoren. Zusätzlich passt Fraunhofer bei Bedarf den Scanner auch an firmenspezifische Sicherheitsanforderungen an.

VUSC unterstützt Unternehmen bei…

- Compliance-Analysen nach CRA (Prüfung der „grundlegenden Cybersicherheitsanforderungen“ aus Annex I)
- der Sicherheitsbewertung fremder Software
- der Qualitätssicherung in der Softwareentwicklung
- der Bewertung von Third-Party-Code und Open Source-Produkten
- Compliance / Datenschutz-Analysen (DSGVO)
- Risk Management
- Due Diligence

Was kann VUSC?

- automatisierte Prüfung von verschiedenen Softwareplattformen:
  - Android
  - iOS
  - Java
  - .net
  - C#, VB.net (aktuell in Entwicklung)
- der Scanner benötigt für seine Analyse keinen Quellcode
- VUSC arbeitet on premises – Software bleibt beim Kunden und muss nicht auf fremde Server geschickt werden
- Übersichtliche Risikoklassifizierung der Schwachstelle
- Genaue Problembeschreibung ermöglicht schnelle Fehlerbebung
- Prüfung von Frameworks

Unsere Leistungen

- Vor-Ort-Installation (on premises)
- Hosted Service auf Wunsch
- Flexibles Lizenzmodell (Mengenstaffelung, kostenfreier Kontroll-Scan nach Fehlerbehebung, etc.)
- Customized Security Analysis: firmenspezifische Anforderungen können in den Scanner integriert werden
- Senior Level Support (direkter Zugang zu Experten-Know-how)
- spezifische Beratung bei Schwachstellenbehebung

Für wen eignet sich VUSC?

- Entscheider in IT-Abteilungen
- Security-Teams von Unternehmen (CERT/SOC)
- Softwareentwickler
- App-Store-/Shop-Betreiber