SICHERHEITSLÜCKEN GEZIELT ENTLARVEN

QUALIFIZIERUNG VON TESTTEAMS AUF ISTQB® CTAL-SEC

Ohne Software-Tests kommen heutzutage weder kommerzielle noch freie Software-Projekte aus. Professionell geschulte Tester prüfen häufig bereits über den gesamten Entwicklungszyklus hinweg Design, Funktionalität und Performance des Software-Systems nach erprobten Verfahren wie zum Beispiel denen des ISTQB®. Die so getestete Software stellt damit zunächst Auftraggeber und Endbenutzer qualitativ und funktional zufrieden.

Allerdings wird von vielen auch nach WannaCry, Spectre und Mirai das Thema Software- und Datensicherheit weiterhin stark vernachlässigt. Wenn an Sicherheitstests gedacht wird, dann meist erst kurz vor dem Software-Release oder wenn es bereits zu spät ist und der öffentlich bekannt gewordene Schadensfall eingetreten ist.

Viele Schwachstellen in Software-Systemen werden häufig zuerst von Kriminellen oder Regierungen gefunden und ausgenutzt. Nach einer Studie der RAND Corporation aus dem Jahr 2017 sind ZeroDay Exploits – also neu entdeckte Schwachstellen in Open- und Closed-Source Software – im Schnitt schon seit sieben Jahren vorhanden. Das bedeutet: Software, die im Jahr 2018 auf den Markt gebracht wird, könnte schon 2025 für den nächsten großen Datenskandal sorgen.
So geschehen Anfang März 2017 bei dem amerikanischen Finanzdienstleister Equifax. Fehlerhaftes Exceptionhandling eines Parsers des Apache Struts-Frameworks ermöglichte es Angreifern, serverseitig beliebige Codes auszuführen und damit auf ca. 145 Millionen personenbezogenen Datensätze zuzugreifen. Der finanzielle Gesamtschaden wird in dreistelliger Millionenhöhe vermutet.

Ein Schwerpunkt des ISTQB® CTAL-SEC beschäftigt sich mit der meistverbreiteten Sicherheitslücke, welche in jedem Unternehmen zu finden ist: dem Menschen.

Nach eigenen Angaben wurde Equifax von der Behörde US-CERT vor dem Einbruch auf diese Sicherheitslücke aufmerksam gemacht. Trotz mehrfacher Versuche konnte das firmeneigene IT-Sicherheitsteam die anfälligen Systeme nicht rechtzeitig identifizieren.

Wie gefährlich unaufgeklärtes Personal und schwache Sicherheitsrichtlinien sein können, zeigen die „Spear Phishing“ Attacken auf Angestellte großer Behörden und Unternehmen im Jahre 2016. Damals wurden von Kriminellen gefälschte Auszahlungsanweisungen, vermeintlich im Namen von CEOs, an Mitarbeiter versendet.
Alleine im Jahr 2016 wurden 50 Fälle von deutschen Unternehmen gemeldet, die Dunkelziffer liegt hier sehr wahrscheinlich deutlich höher. In mehr als der Hälfte dieser gemeldeten Fälle entstanden jeweils Schäden in Höhe von bis zu 40 Millionen Euro.

Aber auch in Europa wird der Schutz von personenbezogenen Daten erst seit Anfang 2018 seitens der Regierungen ernster genommen. Spätestens seit Inkrafttreten der neuen europaweiten Datenschutzrichtlinie GDPR am 25. Mai 2018 kommen die Verursacher solcher Datenskandale nicht mehr mit kleinen Bußgeldern im unteren sechsstelligen Bereich davon. Je nach Ausmaß des Datenlecks können dann – alleine in Europa – Strafzahlungen von bis zu 4% des weltweiten Umsatzes fällig werden. Damit es gar nicht erst zu solch hohen Strafzahlungen kommt, sollten neu entwickelte Software-Systeme sowie firmeninterne Prozesse und Richtlinien auf Sicherheitsaspekte hin getestet werden.

Genau hier setzt das aktuellste Zertifizierungsschema des ISTQB®, der „Certified Tester Advanced Level Security Tester” (CTAL-SEC) an. Tester mit vorhandener „ISTQB® – Foundation Level” Zertifizierung und relevanter Praxiserfahrung können sich in entsprechenden Schulungen zum Sicherheitstester spezialisieren lassen.
In Deutschland gibt es derzeit noch relativ wenige Anbieter für diese Schulung, aber die Notwendigkeit ent-

sprechende Spezialisten auszubilden, wurde mittlerweile erkannt. So bietet das Unternehmen Sogeti Deutschland GmbH als ISTQB®-Partner neben den schon bekannten Schulungen „Test Automation Engineer" oder „Agile Tester" in Kürze auch den „Advanced Level Security Tester" an.

Im Lehrplan des „CTAL-SEC" werden alle notwendigen Aspekte hinsichtlich Sicherheitstests und Optimierung von Sicherheitsprozessen abgedeckt. Thematisch vermittelt dieser zunächst die Grundlagen des Sicherheitstestens, wie die Analyse und Beurteilung von vorhandenen Assets und die Bewertung von Risiken und Sicherheitsrichtlinien, gefolgt von Planung und Umsetzung des Sicherheitstest-Prozesses über den gesamten Entwicklungszyklus von Softwaresystemen hinweg, bis hin zu den nötigen Verfahren und Werkzeugen, die einem Sicherheitstester bekannt sein sollten. Ein Schwerpunkt beschäftigt sich mit der meistverbreiteten Sicherheitslücke, welche in jedem Unternehmen zu finden ist: dem Menschen. Sicherheitstester, die nach „CTAL-SEC" zertifiziert wurden, sind darauf geschult, nach Schwachstellen in firmeninternen Prozessen und Richtlinien zu suchen, diese zu erkennen und gezielte Maßnahmen zu ergreifen.

Abschließend bleibt festzuhalten: Funktionierende Software ist gut – funktionierende und sichere Software ist jedoch besser. Diese Aussage gilt im gleichen Maße für Richtlinien und Prozesse. ■

Mete Boz, Head of Cybersecurity, Sogeti Deutschland

Der Artikel erschien zuerst im SQ-Magazin Nr. 47 | JUNI 2018 **„Security (Testing) in Technik und Gesellschaft"**.

www.sq-magazin.de

Capgemini | sogeti Part of Capgemini

Die neueste Studie zum
Continuous Testing
ist ab sofort erhältlich!

https://www.sogeti.com/ctr2019