Gekommen, um zu bleiben

Wer Software entwickelt, braucht nicht lange auf Hackerangriffe zu warten. Sicher ist nur eins: Jemand wird nach Schwachstellen suchen und sie – sofern vorhanden – ausnutzen. Und zwar nicht nur in öffentlich zugängliche Webapplikationen, sondern in nahezu jeder Anwendung, auch in vermeintlich sicheren Umgebungen. Selbst private Hobbyprojekte stehen unter Beschuss: Jüngere Typo-Squatting-Attacken haben versucht, Ransomware und Crypto-Miner über Paketmanager wie npm und PyPI in Projekte einzuschleusen.

Der Kampf ist unfair: Während eine einzige Schwachstelle für einen erfolgreichen Hack genügt, müssen Teams sowohl ihre komplette Anwendung als auch die Infrastruktur zum Entwickeln, Verteilen und dem Betrieb absichern. Und sie müssen mit dem Unerwarteten rechnen – von Spectre und Meltdown war vor vier Jahren auch sorgfältig geschriebener und getesteter Code betroffen.

Unsere Konferenz zu sicherer Softwareentwicklung heise devSec läuft seit 2017 unter dem Motto „Sichere Software beginnt vor der ersten Zeile Code“, denn die Gefahren lauern im gesamten Software-Lifecycle. Agile Prozesse und Continuous Delivery mit Releases, die im Halbtages- statt Halbjahresrhythmus erfolgen, erfordern eine sorgfältige Integration von Security in die Pipeline. Die Zeiten, in denen das Dev-Team eine Anwendung nach monatelanger Entwicklung dem QA-Team für die Kontrolle übergibt, sind lange vorbei.

Die Aufteilung von Monolithen in Microservices-Architekturen und der Einsatz von Serverless Computing bringen zahlreiche neue Schnittstellen und damit weitere Angriffsflächen mit sich. Das Absichern und Verwalten von Anwendungen für das Internet der Dinge birgt zusätzliche Tücken vom Warten der Firmware über Over-the-Air-Updates bis zum Schutz vor Attacken auf die IoT-Infrastruktur.

Ein zentrales und unverzichtbares Security-Thema ist die Kryptografie, aber die Auswahl der passenden Algorithmen und Tools überfordert viele Entwicklerinnen und Entwickler. Ein prominentes Beispiel sind die wenig durchdachten Konzepte der Luca-App. Dass manche Open-Source-Tools zwar gute Funktionen, aber eine schlechte Dokumentation mitbringen, erschwert den Einsatz. Vermutlich werden zudem Quantencomputer in Kürze die Karten neu mischen und derzeit noch als sicher geltende Algorithmen aufs Abstellgleis schicken.

Das Thema Sicherheit ist, um es mit der Band „Wir sind Helden“ auszudrücken, gekommen, um zu bleiben. Auf Superman und Wonder Woman, die Software ebenso schützen wie Metropolis oder die Paradiesinsel, warten wir vergeblich. Batman wäre vermutlich bereits mit dem Absichern seines Batmobils gegen DoS-Attacken überfordert.

Daher richtet sich dieses Heft an die Alltagshelden, die Software von Schwachstellen befreien: die Softwareentwickler, die Softwarearchitektinnen, die Product Owner und die Security Champions. *iX* und *heise Developer* möchte euch helfen, auch ohne Superkräfte sichere Software zu entwickeln.

RAINALD MENGE-SONNENTAG