InnoSecBW

Cybersecurity-Booster-Bericht
generic.de

generic de
the clean code company

Ein Projekt des

FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe

Gefördert durch das

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Die generic.de software technologies AG ist ein innovatives Unternehmen, das auf die Entwicklung von Individualsoftware im Kundenauftrag spezialisiert ist. Dabei wird großer Wert auf Clean Code gelegt, sodass die Software wartbar und damit nachhaltig ist.

Problemstellung

In einem laufenden Auftrag wird ein komplexes, innovatives System entwickelt, mit dem physische Geräte über eine Cloud-Infrastruktur kontrolliert werden. Die generic.de deckt dabei sowohl die Entwicklung der Cloud-Infrastruktur auf Basis von Microsoft Azure, wie auch die Firmware auf den Endgeräten sowie die Kommunikationskanäle ab. Die Geräte sollen zukünftig in nicht vertrauenswürdigen Umgebungen eingesetzt werden und trotzdem zuverlässig Daten liefern, die Vertraulichkeit der verarbeiteten Daten gewährleisten, sowie einen hohen Schutz gegen Manipulation bieten. Darüber hinaus müssen mögliche Schutzmechanismen gegen den Aufwand für die Administration abgewogen werden, damit eine wirtschaftliche Lösung entsteht. Eine zusätzliche Herausforderung entsteht in der Zusammenarbeit mit Hardwareherstellern, da ein Vendor lock-In vermieden werden muss. Dies schränkt die Auswahl der einsetzbaren Sicherheitsmechanismen ein.

Stand der Kunst und Vorgehen

Im Rahmen des Cybersecurity-Boosters wurden zunächst die einzelnen Anforderungen gesammelt und der Systementwurf gesichtet. Auf dieser Basis organisierte das FZI Forschungszentrum Informatik gemeinsam mit der generic.de einen Workshop, in dem ein ausführliches Threat Modeling, also eine Bedrohungsanalyse, durchgeführt wurde. In diesem Workshop konnten die größten Herausforderungen für das Gesamtsystem sowie die kritischsten Komponenten und Schnittstellen identifiziert werden. Weiterhin konnten die Fachexperten des FZI konkreten Input zum Einsatz von Post-Quanten-Kryptographie und zum Stand der Technik der Absicherung von Hardwarekomponenten geben. Ein Bestandteil des

Workshops war auch die Identifikation relevanter Angreifermodelle, sowie eine Diskussion über den Einsatz etablierter Schutztechnologien in Abwägung zum Entwurf neuer Mechanismen.

Im Nachgang zum Workshop unterstützten die Experten des InnoSecBW-Projekts bei der Auswahl der geeigneten Technologien für die spezifischen Anforderungen an den kritischen Systemkomponenten. Die gute Zusammenarbeit wird auch nach Abschluss des Cybersecurity-Boosters weitergeführt.

Erkenntnisse und Nutzen

Im Rahmen des Cybersecurity-Boosters wurden wichtige Erkenntnisse aufbereitet, die generalisierbar und für die Entwicklung vergleichbarer Systeme anwendbar sind:

Die zukünftige Verfügbarkeit von Quantencomputern wird dazu führen, dass große Teile der heutzutage eingesetzten asymmetrischen kryptographischen Algorithmen gebrochen werden können. Insbesondere bei der Entwicklung von langlebiger Software sowie beim Verarbeiten von Daten, die auch über lange Zeiträume geheim bleiben müssen, ist der Einsatz von **Post-Quanten-Kryptographie** bereits heutzutage sinnvoll. Eine aufwändige Nachrüstung kann so vermieden werden und die Daten bleiben auch langfristig geschützt.

Die **Absicherung von Hardwarekomponenten** in einer nicht vertrauenswürdigen Umgebung stellt eine besondere Herausforderung dar, da potentielle Angreifende jederzeit Zugriff auf die Geräte haben, und diese entwenden und aufwändig analysieren und so Informationen extrahieren können. Daher sollte das Gesamtsystem so konzipiert werden, dass einzelne Geräte kompromittiert werden können, ohne dass die Sicherheit des Gesamtsystems beeinträchtigt wird. So sollten z.B. keine für das Gesamtsystem gültigen Geheimnisse auf den Endgeräten gespeichert sein. Weiterhin sollten Sperrmechanismen vorhanden sein, um gestohlene Geräte aus dem System auszuschließen und unbrauchbar zu machen. Geheimnisse, die auf den Endgeräten liegen müssen, können durch den Einsatz eines Trusted Platform Modules geschützt werden.

Bei der **Auswahl geeigneter Schutzmechanismen** stellt sich häufig die Frage, ob auf bestehende Technologien zurückgegriffen werden soll, oder ob genau abgestimmte Schutzmechanismen selbst entwickelt werden sollten. Bei der Entwicklung von Schutzmaßnahmen besteht ein Ungleichgewicht zum Vorteil der Angreifenden: Für einen Angriff muss nur ein Fehler gefunden werden, zur Absicherung müssen allerdings alle Lücken geschlossen werden. Daher ist es in den allermeisten Fällen empfehlenswert, gut untersuchte, bestehende Technologien einzusetzen und ggf. das eigene Produkt für die Nutzung anzupassen.

Insgesamt konnte das FZI Forschungszentrum Informatik die generic.de im Rahmen des InnoSecBW Cybersecurity-Boosters dabei unterstützen, ein noch sichereres Gesamtsystem zu konzipieren und zu entwickeln. Das innovative Produkt der generic.de konnte so mit modernen Sicherheitstechnologien für einen Einsatz in einer herausfordernden Umgebung abgesichert werden.