Nur sichere Software ist gute Software

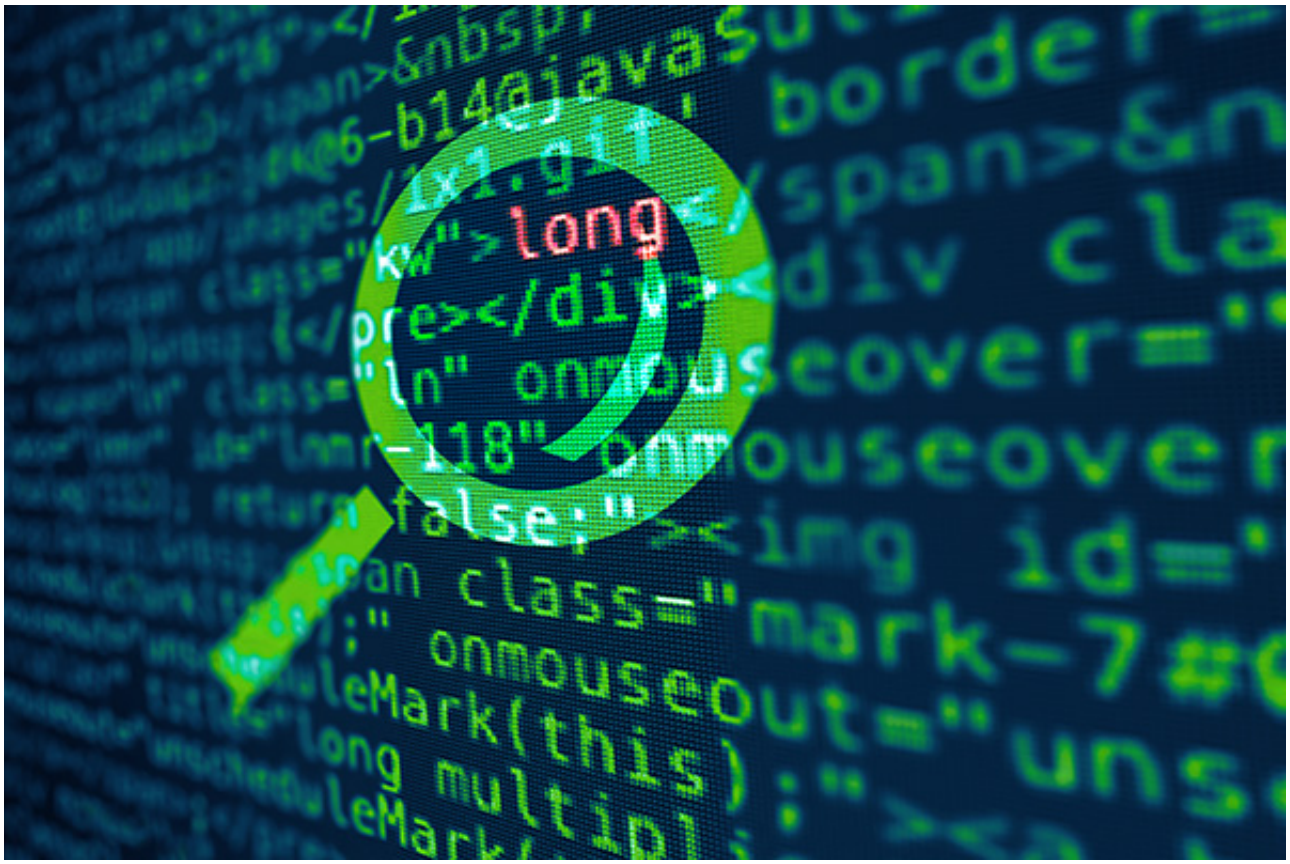
21.09.2021, Produkt-Blog

Die sensiblen Sozialdaten einer Krankenkasse brauchen höchste Sicherheit und besten Schutz. Beides ist Maßstab für alle Produkte, die wir für unsere Kunden entwickeln. Dies zu garantieren, war das Ziel von Entwickler und Software-Architekt Carsten von Schwichow in seinem Ende Juni abgeschlossenen

Projekt zur IT-Security. Ausgangspunkt bei Projektbeginn Oktober 2019 war die Frage: „Was müssen wir in der Entwicklung tun, damit die Produkte sicher sind, die wir herstellen?", erklärt unser Projektleiter. Dabei sollte IT-Sicherheit im gesamten Softwareentwicklungsprozess berücksichtigt werden. Ein Aspekt war, Richtlinien, Werkzeuge und einen Prozess für eine Open-Source-Governance einzuführen. Sie stellt sicher, dass die OS-Komponenten sicher sind und in die Unternehmensarchitektur passen. Dazu gehören die Auswahl der Komponenten, das Lizenzmanagement und die Einschätzung der Sicherheit.

Nutzen und auch Nachteile

Einerseits spart das Nutzen von OS-Komponenten Zeit und Geld, die dann für die fachliche Entwicklung zur Verfügung stehen. Meist werden OS-Komponenten eingesetzt, um mit geringem Aufwand auch komplexe technische Funktionen oder Schnittstellen nutzen zu können. Auf der anderen Seite erfordert ihr Einsatz zwingend das Einhalten von Lizenzbedingungen und wirksame Sicherheitsvorkehrungen. Leichter gesagt als getan. „Es gibt mehrere Hundert Lizenzvarianten", berichtet IT-Security-Experte von Schwichow. Die ständige Weiterentwicklung von OS-Komponenten ist mitunter von Lizenzänderungen begleitet. Das ist noch schwieriger nachzuverfolgen, wenn eine Komponente wiederum andere Komponenten beinhaltet. „Außerdem hatten wir vor ein paar Jahren vielleicht zehn oder zwanzig OS-Komponenten", erinnert sich der IT-Security-Experte. Die Prüfung, ob eine Komponente sinnvoll und problemlos einsetzbar ist, erfolgte in einem manuellen Genehmigungsprozess. „Neue Entwicklungen wie oscare® CX und oscare® connect nutzen allerdings sehr viele OS-Komponenten. Das macht einen automatisierten Prüfprozess unverzichtbar."



Auf Lizenz und Sicherheit geprüft

„Open-Source-Komponenten, die wir in unseren Produkten verbauen, werden jetzt maschinell über die Nexus-Plattform auf Sicherheit und Lizenzen geprüft", berichtet von Schwichow. Dazu muss der Entwickler keinen Antrag mehr stellen. Vielmehr interagiert das Programm, mit dem der Entwickler seinen Quellcode schreibt, mit der Nexus-Plattform. Hat eine OS-Komponente Sicherheitslücken, öffnet etwa Verbindungen oder kann unbemerkt von außen manipuliert werden, signalisiert die Nexus-Plattform diese mit einer roten Ampel. Gibt es keine Alternative zu der Komponente, kommt Jens Trach ins Spiel, seit Juni IT-Security-Spezialist im Geschäftsbereich Entwicklung: „Ich prüfe mit dem Entwicklungsteam, ob die Sicherheitslücke hier für uns relevant ist oder ob wir sie umgehen, abdichten

oder schließen können.” Die Kriterien für den Ausschluss einer Komponente sind in der Nexus-Plattform hinterlegt. Dabei folgen wir den Empfehlungen des Herstellers, nehmen aber auch eigene Anpassungen vor. „Diese legt das Policy Board fest, ein Gremium mit Vertretern aus Lizenzmanagement, Unternehmensarchitektur und Security sowie dem Informationssicherheitsbeauftragten”, sagt von Schwichow. Ein grundsätzliches Ausschlusskriterium ist beispielsweise eine Copyleft-Lizenz, die dazu verpflichtet, auch den Quellcode unseres Produkts offenzulegen, in das die Komponente integriert werden soll. „Verletze ich das Urheberrecht, können sich daraus üble Konventionalstrafen ergeben”, warnt Trach. Die Entwicklungsteams können dadurch aber selbstständiger und schneller arbeiten, weil sie nicht auf das Go anderer Abteilungen warten müssen, um eine Komponente zu testen oder in ihre Anwendung einzubinden. Unsere Produkte sind sicherer, weil Verstöße der OS-Komponente gegen die festgelegten Kriterien unmittelbar angezeigt und Hilfestellungen zur Korrektur angeboten werden.

Autor/in: