Mit zunehmender Vernetzung im Alltag steigen die Anforderungen an Sicherheit. Foto: iStock/mikkelwilliam

Vernetzung als Herausforderung

Immer mehr Produkte des täglichen Gebrauchs sind ständig mit dem Internet verbunden. Was uns vielfach das Leben erleichtert, schafft für die Hersteller neue Herausforderungen.

Das „Internet der Dinge" schafft für Unternehmen große Chancen. Dabei müssen sie aber auch den Sicherheitsaspekt mitdenken – daran erinnert Prof. Ruth Breu vom Institut für Informatik.

Der Kühlschrank meldet, dass keine Milch mehr da ist, die Klimaanlage zu Hause lässt sich aus dem Büro via Internet steuern, das Auto ruft man vor der Abfahrt mittels Knopfdruck aus der Garage, es wartet vor der Tür, und über den vernetzten Herzschrittmacher wissen Ärzte genau, wie es der Patientin geht: Wir leben in einer zunehmend vernetzten Welt.

In den nächsten Jahren werden Anwendungen und Produkte auf den Markt kommen, die durch Vernetzung einiges bequemer machen – das „Internet der Dinge" ist aber auch ein potenzielles Einfallstor für Angreifer von außen. „IT-Systeme werden immer komplexer, dementsprechend wird auch die Wartung immer aufwändiger, vor allem, wenn die Systeme vor Attacken von außen abgesichert werden müssen", sagt Prof. Ruth Breu, Leiterin des Instituts für Informatik und der Arbeitsgruppe „Quality Engineering" an diesem Institut. Ihre Arbeitsgruppe beschäftigt sich un-

ter anderem mit dem komplexen Zusammenspiel von Sicherheit und Qualitätsmanagement bei IT-Produkten: „Sie können sich ein IT-System wie ein Haus vorstellen: Das Haus ist auch nur dann sicher, wenn alle Fenster und Türen geschlossen sind – alle geschlossenen Fenster nützen nichts, wenn die Kellertür offen ist. Bei komplexen Systemen reden wir hier aber von hunderttausenden Fenstern, deren Position im Haus sich regelmäßig ändert und bei denen manche Fenster sich automatisch ebenfalls öffnen, wenn andere aufgehen und umgekehrt. Über all das muss jemand, der für die Sicherheit verantwortlich ist, den Überblick bewahren."

Komplexität vereinfachen

Innerhalb von Unternehmen treffen hier Aufgabengebiete aufeinander, die auf Deutsch beide mit „Sicherheit" übersetzt werden: Safety und Security. Mit Safety ist die Bedienungs- und Betriebssicherheit eines Produkts gemeint: Etwa, dass eine implantierte Insulinpumpe keine Fehlfunktionen aufweist, die das Leben des Patienten gefährden, oder, dass ein Airbag nur im Notfall auslöst. „Safety-Eigenschaften eingebetteter Software-Systeme sind heute gut beherrschbar – entsprechende Software ist in sicherheitskritischen Produkten wie Flugzeugen, Kraftfahrzeugen, im Schienenverkehr oder in Medizinprodukten seit Jahrzehnten im Einsatz", erläutert Ruth Breu. Neu ist die Verknüpfung mit Security: Die Sicherung vor Angriffen, die von außen kommen. „Für viele Unternehmen ist dieser Aspekt sehr neu, sie können damit noch nicht richtig umgehen – Security kann in den neuen vernetzten Anwendungen nicht ohne Safety gedacht werden und umgekehrt." Außerdem spielen daneben auch Aspekte wie der Schutz von Kundendaten und Privatsphäre eine wichtige Rolle.

Um es IT-Verantwortlichen leichter zu machen, den Überblick über unterschiedlichste Sicherheits-Anforderungen zu bewahren, haben Ruth Breu, Michael Brunner und Christian Sillaber eine eigene Softwarelösung entwickelt. „Unternehmen dokumentieren heute noch zu oft komplexe Zusammenhänge über einfache Excel-Tabellen – dass das sehr schnell sehr unübersichtlich und fehlerhaft ist, wird niemanden wundern", erklärt sie. Die Software heißt Adamant; sie kann je nach Unternehmen entsprechend angepasst werden und ermöglicht es unter anderem, für jede Aufgabe auch Abhängigkeiten einzutragen, außerdem Wartungsintervalle festzulegen und alle Aufgaben nach Prioritäten zu reihen. „So entsteht statt einer Liste ein Netz, das tatsächliche Anforderungen viel besser abbildet und es auch möglich macht, Schnittstellen und Abhängigkeiten etwa zwischen Safety- und Security-Anforderungen abzubilden. Gerade Software wird ja ständig weiterentwickelt und Updates während des Produkt-Lebenszyklus sind nicht mehr nur für Smartphones und Computer selbstverständlich, sondern auch zunehmend für Autos, Produktionsanlagen und eine große Zahl weiterer Gegenstände und Produkte, die wir täglich nutzen. Wenn in einem Update eine Komponente geändert wird, bildet unser System konkret ab, welche weiteren Komponenten dadurch betroffen sind und wo sich dadurch zum Beispiel neue

«Unternehmen müssen die Sicherheit ihrer Produkte gleich von Anfang an mitdenken.»

Ruth Breu Foto: Fotogräfin Claudia Bachlechner

Lücken ergeben", sagt die Informatikerin. So sei auch möglich, bestimmte Bereiche in regelmäßigen Abständen automatisch kontrollieren zu lassen, während für andere, sicherheitsrelevantere Teile Erinnerungen für eine manuelle Kontrolle durch einen Mitarbeiter eingestellt werden können. „Mit Adamant schaffen wir es, alle nötigen Sicherheitsaspekte abzubilden und ermöglichen Unternehmen so einen vollständigen Überblick über alles, was sie beachten müssen. Ein großer deutscher Automobilhersteller hat schon Interesse daran bekundet."

Zukunft

Adamant soll jedenfalls weiterentwickelt werden, dazu laufen derzeit mehrere Projektanträge, an denen auch Unternehmenspartner beteiligt sind. Sicher ist: Die Anforderungen an die Sicherheit softwareintensiver Produkte werden in Zukunft weiter steigen, nicht zuletzt bei jenen Produkten, die bisher nicht vernetzt waren und deshalb nicht vor Angriffen von außen geschützt werden mussten. „Mit der Vernetzung steigen die Anforderungen. Deshalb ist es für Unternehmen in Zukunft unverzichtbar, die Sicherheit ihrer Produkte vor Angriffen von außen und innen gleich von Anfang an mitzudenken", sagt Ruth Breu. In Anbetracht der kommenden Digitalisierungswelle ist das Etablieren von Prozessen für IT-Sicherheit ein wichtiger Faktor für den Erfolg am Markt.

stefan.hohenwarter@uibk.ac.at

Die von Ruth Breu, Michaeal Brunner und Christian Sillaber entwickelte Software ermöglicht auch die Darstellung komplexer Abhängigkeiten. Foto: iStock/BlackJack3D