VDI nachrichten
Donnerstag, 16. März 2017, Ausgabe Nr. 11

IT-SICHERHEIT

Datenschutz mit Mehrwert

Von Kathleen Spilok | 16. März 2017 | Ausgabe 11

LETZTER NÄCHSTER

Wibu-Systems schützt vernetzte Maschinen vor Hackern und erleichtert Nutzern gleichzeitig den Umgang mit Software-Lizenzen.

Foto: Wibu Systems

Oliver Winzenried, Chef der Wibu-Systems AG, sieht vielfältige Aufgaben in der IT-Sicherheit.

Anlässe gibt es genug, um beim Thema Software- und Datensicherheit die Ohren zu spitzen. Oliver Winzenried, Chef von Wibu Systems, weiß warum: „Bei uns in Europa hängen Wirtschaft und Wohlstand stark von der IT-Sicherheit ab.“ Sein Unternehmen in der Karlsruher Südstadt entwickelt Schutz- und Lizenzierungssysteme für Maschinen- und Gerätehersteller. Vor knapp 30 Jahren, als es noch selbstverständlich war, unter Freunden Musikhits als Raubkopien auf CDs und Kassetten weiterzureichen, setzte Winzenried einen frühen Kontrapunkt: Er arbeitete an Verfahren zum Kopierschutz für PC-Software. So entstand die heutige Wibu-Systems AG, benannt nach den Gründern Oliver Winzenried und Marcellus Buchheit.

Landkarte Industrie 4.0

Heute ist die Welt eine andere und auch Wibu-Systems hat sich verändert. Alles dreht sich um Industrie 4.0, eine extreme Herausforderung für die Sicherheit. Maschinen, Geräte, Steuerungen, Autos – alles wird miteinander vernetzt, Angriffe auf Unternehmen und Netze finden immer mehr Ziele.

Wie Sicherheitslösungen für Industrie 4.0 aussehen? „Wir denken: Jede vernetzte Komponente muss sich ausweisen können“, sagt Winzenried. Damit beim Datenaustausch Sender und Empfänger nachprüfen können, dass sie wirklich mit dem Richtigen sprechen, die Daten unterwegs nicht abgegriffen oder manipuliert wurden. Und: „Die Sicherheitssysteme müssen auch vor Fehlbedienungen einen Schutz bieten“, findet der Unternehmer. Unter Sicherheit versteht er: Schutz vor unberechtigter Veränderung, für Daten genauso wie für Software.

Wibu-Systems AG

In all der Vielfalt von IT-Sicherheit hat sich die Firma Wibu eine Nische geschaffen, in der sie sich auf spezielle Schutzmechanismen konzentriert. Ein Beispiel sind kryptografische Verfahren der Verschlüsselung, um schützenswerte Informationen für Unberechtigte unlesbar zu machen. Dazu kommen der Schutz vor dem Nachbau von Geräten oder Maschinen, den Experten „Reverse-Engineering“ nennen, und der Schutz vor Manipulation. Außerdem gehören Lizenzierungen dazu. „Damit lassen sich bestimmte Funktionen auf einer Software für zahlende Nutzer freischalten“, erklärt Winzenried. Auf diese Weise kann ein Anbieter regelmäßige Einnahmen generieren.

„Wir tun uns leichter, wenn wir neben der Sicherheit noch Lizenzierungen als Zusatznutzen anbieten können“, unterstreicht er. Beispielhaft ist für den Unternehmer das Auto der Zukunft. „Stellen Sie sich vor, Ihr Auto fährt im Alltag mit 70 PS und am Wochenende wollen Sie mit 120 PS unterwegs sein.“ Mit flexiblen Lizenzen ließe sich über das Onlineportal des Fahrzeugherstellers dann eine höhere Leistung für zwei Tage freischalten. Leistungssteigerung auf Knopfdruck, „so was gibt es schon bei Medizingeräteherstellern“, berichtet er.

Sicherheit hat allerdings ein Wahrnehmungsproblem. „Die Technik funktioniert nämlich auch ohne die Sicherheitskomponente“, argumentiert der Wibu-Chef. Wie viele Attacken man mit installierter Sicherheit tatsächlich abwehren kann, darüber gibt es keine genauen Angaben. „Als der Computerwurm Stuxnet im Jahr 2010 die Siemens-Steuerung einer Uranaufbereitungsanlage im Iran angegriffen hat, hat das sicherlich die Aufmerksamkeit erhöht“, meint er. Für überaus gefährlich hält er kleine Manipulationen à la Stuxnet, die ein Anlagenbetreiber nicht gleich bemerkt. Auch dafür hat er ein Beispiel: Wenn sich in der Automobilindustrie ein Wettbewerber oder ein Erpresser in die Lackierprogramme einhackt und die Dicke der Lackschicht halbiert. „Das sieht man nicht sofort, aber nach zwei Jahren fängt das Auto an zu rosten, weil der Lack zu dünn war“, führt er aus. Eine Katastrophe für den Hersteller.

Auch für das Unternehmen ist es nicht leicht, wahrgenommen zu werden. Man sieht nicht, wo Wibu-Technologie drinsteckt. Sie ist immer in Geräten, Maschinen, Komponenten eingebaut. Ein bisschen sehen und anfassen lassen sich die Systeme trotzdem, beispielsweise in der kleinen Produktion im Erdgeschoss des dreistöckigen Firmengebäudes. Hier kommt die Sicherheit wahlweise auf einen speziellen USB-Stick, eine Speicherkarte oder auf 5 mm x 5 mm große Smartcard-Chips. Nur ein kleiner Druckluftseufzer ist zu hören, wenn ein automatischer Greifarm die Sticks und Chips mit der Sicherheitssoftware impft. „Reine Softwaretools verkaufen wir an Hersteller, die einen vorhandenen Sicherheitsanker ergänzen wollen“, fügt er hinzu.

Tüfteln unter dem Firmendach ist das eine. Das andere ist der Austausch mit anderen. Das Forum, in dem er und Kollegen aus der Industrie Herausforderungen Zeitalter der Digitalisierung diskutieren und angehen, ist die Plattform Industrie 4.0. Seit 2013 ist Winzenried dabei. Damals startete die Zusammenarbeit der Verbände Bitcom, ZVEI, VDMA unter dem Dach der Acatech. Ein wichtiger Kreis, in dem Sicherheit eine angemessene Rolle spiele, findet Winzenried. Vor zwei Jahren hat das Bundeswirtschaftsministerium die Initiative in eine politische Plattform überführt und die Gewerkschaft beteiligt. Das sei sinnvoll. „Die Arbeitsbedingungen werden sich ändern, da muss der Mensch mitgenommen werden“, betont Winzenried, der die Plattform für ihre gute Arbeit lobt.

Was wichtig ist, um vorwärtszukommen? Die Aufmerksamkeit der Politik, internationale Standards,

viel Forschung und keine Handelshemmnisse, stellt der Wibu-Mann fest. Und: Zu ausführlich würden in Deutschland Risiken und Nebenwirkungen erkundet, zu lange Spezifikationen geschrieben, bevor ein Produkt entwickelt werde. „Viel früher schon mit einem ersten Ergebnis auf den Markt gehen, Produkte so gestalten, dass sie sich leicht in alle Richtungen erweitern lassen und viel früher das Feedback einsammeln“, lautet daher sein Lösungsvorschlag.

„100 % Sicherheit gibt es nicht“, sagt Winzenried im Gespräch öfter. Dass man trotzdem den Kopf nicht in den Sand stecken muss, will er auf der diesjährigen Hannover Messe beweisen. Er wird Hacker auffordern, sein Schutzsystem anzugreifen, das auf der neuen Verschlüsselungsmethode Blurry-Box beruht und das alle Schutzmechanismen offenlegt. Trotzdem rechnet er nicht damit, dass das jemand schafft. Der Aufwand, den Schutz zu umgehen, ist genauso hoch, wie die Anwendung neu zu entwickeln. Dennoch – ein Restrisiko bleibt.ciu

Letzter Artikel

Nächster Artikel

Offene Standards im Gebäude

Leichtbausysteme sind schwer zu simulieren

STELLENANGEBOTE

MEHR