DIGITALISIERUNG IM MITTELSTAND

Kleine und mittelgroße Unternehmen sehen der Digitalisierung oft mit gemischten Gefühlen entgegen. Dabei gibt es durchaus Wege, auch in einer vernetzten Welt die Hoheit über die eigenen Daten zu behalten – und damit jede Menge neuer Geschäftsmodelle auszuloten. Nicht nur Gerätehersteller Miele und der Bayrische Rundfunk machen das vor.

Fort Knox für die Industrie

DIGITALE SOUVERÄNITÄT

Unternehmen kämpfen um ihre Datenhoheit. Sichere IT-Systeme sollen die Abhängigkeit von den Webriesen in den USA und Asien reduzieren.

Manchmal, sagt Hans-Joachim Popp, fühle er sich wie ein Querdenker. Jetzt zum Beispiel, da er die Giganten der IT-Branche attackiert. Die nämlich, so empört sich der 58-Jährige, der als Chief Information Officer auch für die IT-Sicherheit beim Deutschen Zentrum für Luft- und Raumfahrt (DLR) in Köln verantwortlich ist, schieben ein großes Problem seit Jahren vor sich her. „Wichtige Komponenten des Netzverkehrs und vor allem auch die Datenbanken sind bei Weitem nicht sicher genug aufgebaut. Die Marktführer sehen dazu bisher auch gar keine Veranlassung“, sagt Popp. Selbst ihre großen Kunden behandeln Konzerne wie Cisco, Microsoft oder Oracle wie kleine Bittsteller. Für Popp gibt es nur einen Ausweg: „Schon um in der Diskussion auf Augenhöhe zu bleiben, müssen wir in Europa selbst in der Lage sein, sichere IT-Systeme zu bauen.“

Popp schimpft nicht nur. Er tut auch etwas. In einem besonders sensiblen Bereich des DLR hat er die Router des Marktführers Cisco aus seinem Netz rausgeworfen und Produkte des deutschen Konkurrenten Lancom Systems eingebaut. 200 Geräte sichern die besonders häufig von Hackern und Geheimdiensten angegriffenen Rechner der internen IT-Administratoren ab. Popp ist der erste Chief Information Officer in Deutschland, der so einen Wechsel öffentlich macht. Gemessen an der Marktmacht des amerikanischen Konzerns Cisco, ist der deutsche Konkurrent Lancom ein Winzling. Doch genau dies war für Popp einer der wichtigsten Gründe für den Schritt: „Als europäische Nutzer müssen wir dafür sorgen, dass es eine europäische Alternative zu den Marktführern gibt.“ Lancom sei ein „Hidden

ILLUSTRATION: KATI SZILÁGYI

Champion“, dessen Technik man in den Ausschreibungen berücksichtigen müsse. „Nutzen wir dies nicht, geht dieses wertvolle Know-how langfristig wieder verloren.“

Zwar hatte die Bundesregierung, nachdem der ehemalige NSA-Mitarbeiter Edward Snowden über das massenhafte Ausspähen berichtet hatte, die deutsche Wirtschaft aufgerufen, „verstärkt vertrauenswürdige Produkte von Herstellern aus Deutschland und Europa einzusetzen“. Doch bisher satteln nur wenige um. Trotz aller Einfallstore für Spionage- und Cyberangriffe ist es bequemer, bekannte Produkte in die IT-Systeme einzubauen. Die Sicherheitsrisiken finden dann kaum noch Beachtung.

Nur wenige Experten prangern diese Naivität so lautstark an wie Lancom-Chef Ralf Koenzen. „Blindes Vertrauen in die am Markt verfügbaren Lösungen und das Ausblenden möglicher Risiken sind mehr denn je fehl am Platze. Denn welche Sicherheitslücken und Hintertüren selbst bei namhaften IT-Konzernen absichtlich oder unabsichtlich eingebaut wurden, kann niemand feststellen.“

Fast alle großen IT-Anbieter stehen unter dem Generalverdacht, eng mit ihren nationalen Geheimdiensten zusammenzuarbeiten, um Daten abzusaugen. US-Konzerne wie Microsoft, Google und Cisco unterhalten offenbar enge Verbindungen zu den US-amerikanischen Nachrichtendiensten, wie die Snowden-Dokumente zeigten.

Einen ähnlichen Schulterschluss unterstellt die US-Regierung aufstrebenden IT-Nationen wie China und Russland – und sieht darin eine „Gefahr für die nationale Sicherheit“. Produkte des chinesischen IT-Konzerns Huawei dürfen in den Vermittlungsstellen US-amerikanischer Mobilfunk- und Festnetzbetreiber nicht mehr eingesetzt werden. Die Sorgen sind durchaus berechtigt. Huawei entstand quasi im Regierungsauftrag und verdankt seinen Aufstieg bis heute staatlichen Subventionen in Milliardenhöhe, die aggressive Discountangebote bei Ausschreibungen erst ermöglichen.

Embargo in den USA

Genauso hart geht die US-Administration jetzt gegen den russischen IT-Sicherheitsanbieter Kaspersky Labs vor. Wegen enger Verbindungen zu russischen Regierungsstellen hat US-Präsident Donald Trump den Einsatz von Kaspersky-Produkten in US-Behörden vor zwei Wochen verboten. Die Bundesregierung verzichtet bislang auf ein Handelsembargo für sicherheitsrelevante IT-Komponenten. Vor allem Chinas IT-Konzern Huawei gewinnt deshalb in Deutschland weiter Marktanteile auf Kosten seiner europäischen Konkurrenten Nokia und Ericsson. Die Deutsche Telekom baut Huawei-Technik im großen Stil in ihren Netzen ein. Auch Vodafone und Telefónica gehören zu Huaweis Topkunden.

So sehr sich deutsche Unternehmer wie der DLR-Mann Popp mit sicherer Technik auch vor Hackern und Spionen abzuschirmen versuchen: Dies ist nur der erste Schritt zur digitalen Souveränität. Genauso wichtig ist die Hoheit über all die Daten zu Abläufen in der Produktion oder den Gewohnheiten von Kunden. Denn sie sind der wertvolle Rohstoff, aus dem sich neue Geschäfte entwickeln lassen. Und sie versucht die deutsche Industrie derzeit immer stärker vor dem Zugriff der Internetkonzerne zu schützen. So wollen die hiesigen Firmen verhindern, dass Google und Amazon, Apple und Facebook ihre Algorithmen mit diesen Daten füttern – und irgendwann auch die passenden Dienste anbieten.

Initiativen für sichere Datenräume

Die Autohersteller Daimler, BMW und Audi gehörten zu den ersten, die diese Gefahr erkannten: Vor zwei Jahren haben sie für rund 2,8 Milliarden Euro den Straßenkartendienst Here gekauft. Er soll eine eigene Plattform für Fahrzeugdaten bauen, damit sie mit den eigenen Bewegungsprofilen die künftig autonom rollenden Fahrzeuge steuern können.

Einer ähnlichen Logik folgt ein staatlich gefördertes Bündnis. Industriekonzerne wie Thyssenkrupp, Salzgitter, Volkswagen sowie der Sensorhersteller Sick AG und der IT-Konzern Atos gründeten Anfang 2016 mit der Fraunhofer-Gesellschaft den branchenübergreifenden Industrial Data Space (IDS). Das Ziel ist der Aufbau eines sicheren Datenraumes, in dem die Mitglieder selbst bestimmen können, wer die dort abgelegten Daten in welcher Form benutzen darf. In einem ersten Projekt zeigt Thyssenkrupp, wie sich aus den Verkehrs- und Bewegungsdaten von Spediteuren die Ankunftszeit von Lkws genau vorhersagen lässt.

Mit dem IDS wollen die inzwischen 80 Mitglieder die Grundlagen für ein sicheres und vertrauenswürdiges Internet schaffen. „Inzwischen haben alle Unternehmen verstanden, dass Daten einen Wert haben und die Kombination aus Daten einen noch höheren Wert besitzt“, sagt Reinhold Achatz, Vorstandsvorsitzender der Industrial Data Space Association und Innovationschef beim Essener Industriekonzern Thyssenkrupp. „Deshalb wollen wir Unternehmen mit dem Industrial Data Space sicheren Datenaustausch zur Verfügung stellen.“ Ein Fort Knox für die deutsche Industrie soll daraus entstehen.

Der Fehler aus Zeiten, als es noch darum ging, Verbraucher übers Internet zu verbinden, und noch nicht darum, die Produktion zu vernetzen, soll sich nicht widerholen. Das Geschäftsmodell von Google, Facebook und Co. baut darauf auf, dass Konsumenten ihre Daten preisgeben. „So einen Kontrollverlust wollen die Unternehmen nicht“, sagt Achatz. „Lösen lässt sich das Problem deshalb nur, wenn ich Daten Partnern zur Verfügung stelle, ohne dass ich meine Rechte als Eigentümer verliere.“ Jeder noch so kleine Datensatz bekommt im Industrial Data Space einen Vertrag, der die Nutzungsrechte exakt festlegt und auch die Einhaltung überwacht.

Weltstandard aus Deutschland

Die Vision von Achatz: In Deutschland steht die Wiege für einen neuen Weltstandard, der den Datenaustausch zwischen vertrauenwürdigen Partnern absichert. Deshalb drängt der IDS-Chef die Mitglieder, den Industrial Data Space auch für Unternehmen aus den USA und aus Asien zu öffnen. Eine Gratwanderung: Chinas umstrittener IT-Riese Huawei nahm die Einladung sofort an und unterstützt das Projekt, obwohl das umstrittene Unternehmen nach Ansicht einiger Mitglieder den Status „vertrauenswürdig“ nicht verdient. ■

„Wir müssen in Europa selbst in der Lage sein, sichere IT-Systeme zu bauen“

Hans-Joachim Popp, CIO beim Deutschen Zentrum für Luft- und Raumfahrt

juergen.berke@wiwo.de

ILLUSTRATION: KATI SZILÁGYI