

Sicherheit ist das Maß aller Internetdinge

Globale Datennetze haben sich zu riesigen Marktplätzen für den Austausch von Informationen und Waren entwickelt. Nun werden sie auch Sammelbecken für Fertigungsdaten. Produziert wird auf Kundenwunsch - vorausgesetzt, die Netze sind sicher.

Von Stephan Finsterbusch

FRANKFURT, 2. Juli.

Ralf Koenzen hat es in der Hand: ein amtliches Zertifikat für das Produktpotfolio des Unternehmens. Seine kleinen Kisten haben eine große Wirkung. Sie sind nicht nur Knotenpunkte der digitalen grenzüberschreitenden Kommunikation. Die sogenannten Switches und Routers für die Steuerung des Datenverkehrs im Internet der Lancom Systems GmbH sind auch zweieinhalb Jahre lang reiflich getestet und behördlich geprüft worden. Heute gelten sie als so sicher, wie es in der Branche nur irgendwie geht - und das ist in der Welt der Computer viel wert.

Das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) gab ihm das alles schwarz auf weiß. "Klar", sagt er, "hundertprozentige Sicherheit gibt es nie, aber wir kommen schon nah ans Ideal heran." Koenzen hat einiges im Griff und vieles unter Kontrolle. Lancom ist hierzulande nach der amerikanischen Cisco-Gruppe der zweitgrößte Anbieter für die digitalen Wegweiser im Internetverkehr. Es hat keine allgemein zugängliche Software wie so viele der Konkurrenten; das lässt seine Geräte sicherer erscheinen. Lancom arbeitet mit einem eigenentwickelten Betriebssystem, setzt auf deutsche Produktion, auf deutsche Qualität und nun auch auf ein deutsches Zertifikat.

"Made in Germany" hat auch in Fragen sicherer Informationstechniken (IT) einen guten Ruf. Damit geht Koenzen von der Unternehmenszentrale im westdeutschen Würselen bei Aachen nun auf landesweiten Expansionskurs. Denn die klassisch deutschen Industrien machen sich unter Slogans wie "Internet der Dinge" oder "Industrie 4.0" gerade fit für das Datenzeitalter. Sie digitalisieren ganze Produktionsstätten.

Auto- und Maschinenbauer verfolgen neue Produktionskonzepte; Chemie- und Pharmaindustrien bauen neuartige Fertigungsstrecken auf. Ohne Computer, Software und Datenanalysen geht da nichts mehr. "Informationen sind heute essentiell für den Geschäftserfolg", erklärt Derk Fischer vom Beratungshaus Pricewaterhouse Coopers (PWC). "Mit zunehmender Digitalisierung und globaler Vernetzung steigen auch die Gefahren für die Informationssicherheit", sagt Hans-Günter Börgmann, Geschäftsführer des Dokumentenverwalters Iron Mountain Deutschland.

Vor dem Hintergrund der jüngsten Aufdeckungen rund um digitale Wirtschafts- und Datenspionage, Angriffe auf Netzwerke von Unternehmen, Forschungs- und Entwicklungseinrichtungen sind Konzernlenker, Unternehmer und staatliche Behörden alarmiert. Nichts scheint im Zeitalter binärer Datenberge, gigantischer Rechenzentralen, permanenter Hackerangriffe und institutionell organisierter Überwachungsmaßnahmen mehr unmöglich zu sein - im Guten wie im Bösen.

Der Schaden digitaler Angriffe wird von der internationalen Polizeiorganisation Interpol auf mehrere Billionen Euro im Jahr geschätzt. Allein in Europa soll er sich auf 750 Milliarden Euro im Jahr belaufen. Dieses Ausmaß lässt die Nachfrage nach gesicherten IT-Anlagen kräftig wachsen - von den kleinen weißen Schaltkästen für die großen Reisen durch die Welt des Internets bis hin zu den kühlenschrankgroßen Netzwerkrechnern und den Datenzentren vom Ausmaß einer Sportarena.

"Digitale Sicherheit ist das große Thema der Stunde", sagt Dieter Kempf, Präsident des deutschen IT-Branchenverbandes Bitkom in Berlin. Das werde es wohl auch noch eine Zeitlang bleiben. Um von den Vorteilen der modernen Technik profitieren zu können, müssten die Anwender Vertrauen haben, dass ihre Daten sicher seien, erklärt BSI-Präsident Michael Hange in einer E-Mail. Dieses Vertrauen sei nur herzustellen, wenn es unabhängige, transparente und international anerkannte Standards gebe. Doch von solchen grenzübergreifenden Standards ist die Politik noch weit entfernt.

So arbeiten die Unternehmen an ihren eigenen Netzwerken. Mit der sogenannten Industrie 4.0 machen sich das verarbeitende Gewerbe wie der Auto-, Werkzeug- und Maschinenbau, die Chemie oder die Pharmazie daran, die Automatisierung ihrer Produktion auf eine neue Stufe zu stellen. Während heute eine Fertigung von zentraler Stelle aus geleitet, reguliert und kontrolliert wird, soll die Produktion künftig über dezentrale autonome Entscheidungszentren gesteuert werden; während es in Fertigungsanlagen heute oft darum geht, genau definierten Standards zu folgen, möglichst effizient eine möglichst große Zahl gleichartiger Teile herzustellen, wird die Produktion künftig individueller ausfallen. Jeder Kunde hat einen etwas anderen Wunsch, jeder Wunsch soll erfüllt werden, Angebot folgt Nachfrage, Technik macht es möglich.

Dafür werden alle Komponenten einer Produktionskette über Sensoren, Chips und Prozessoren miteinander verbunden. Sie können sich so aufeinander abstimmen, selbst regulieren, kontrollieren und justieren. Jedes Teil weiß, welche Daten es braucht, wo es sie aus dem System bekommt und wie es sie einsetzt. Programmierung ist alles. Jede Komponente ist Teil eines Netzwerkes, ist kommunikationsfähig und kann mit anderen Teilen in- und außerhalb des Systems Daten austauschen. In der deutschen IT-Branche wurde dafür der Begriff vom "Internet der Dinge" geprägt. Ein Netzwerk der Zukunft.

Solche Datennetze sollen hochflexible Fertigungsstrukturen entstehen lassen. Diese Flexibilität kann es den Produzenten dann ermöglichen, auf individuelle Kundenwünsche einzugehen, ohne Größen- und Kostenvorteile einzubüßen. Der Produktionstechniker Michael Höing, Leiter der Abteilung Elektronik der Weidmüller Interface GmbH & Co. KG, umschrieb es in einem Interview einmal so: "Die klassische Automatisierungspyramide wird abgelöst durch ein Netzwerk." Die Stichworte der Zukunft seien Wandlungsfähigkeit, Informationsaustausch, Flexibilisierung - und vor allem Sicherheit. Es geht um hochsensible Daten und Informationen, um Identität und Integrität, Authentifizierungen und Zugangsberechtigungen, Manipulationssperren, Firewalls und Sicherheitsscanner.

Quasi eine abhörsichere Kommunikation zwischen Maschinen. "In sensiblen Bereichen müssen hier Sicherheitswerkzeuge eingesetzt werden, die den Vorgaben des BSI entsprechen", sagt Ralf Koenzen von Lancom Systems.

Das in Bonn ansässige BSI gibt nicht nur den Grundschutzkatalog mit Empfehlungen für Maßnahmen zum Schutz für IT-Systeme heraus, es testet die Sicherheit von Systemen und erstellt für die Tests auch Zeugnisse. Dabei steht derzeit vor allem die zentrale Erfassung, Speicherung und Verarbeitung von Daten, das sogenannte Cloudcomputing, ganz oben auf der Tagesordnung der Sicherheitsexperten. Unternehmen wie die Softwareschmieden SAP, Microsoft oder Oracle haben Milliarden von Euro in den Aufbau einer eigenen Cloudstruktur investiert. Sie können den Kunden so quasi Software und IT-Dienstleistungen aus der Steckdose anbieten, deren digitalisierte Daten aller Art erfassen, speichern und verarbeiten. Hundertprozentig sichern können sie die Informationen allerdings nicht. Das BSI sieht hier dringenden Handlungsbedarf und arbeitet unter Einbeziehung der Wirtschaft an entsprechenden Grundschutz-Bausteinen.

Darüber hinaus gründete das Bundesamt im vergangenen Jahr mit dem Branchenverband Bitkom die Allianz für Cyber-Sicherheit - eine Initiative, welche die Cyber-Sicherheit in Deutschland erhöhen und die Widerstandsfähigkeit des Standortes gegenüber Angriffen im Internet stärken soll. Die Allianz richtet sich an hiesige Unternehmen und Behörden, Institutionen und Organisationen. Nach

den Worten von Bitkom-Präsident Kempf gehören derzeit fast 300 Unternehmen dieser Allianz an.

Für Lancom-Chef Ralf Koenzen ist in Fragen der Sicherheit das BSI momentan das Maß der Dinge. "Wir haben uns mehr als zwei Jahre den BSI-Prüfungen unterzogen, wurden mit unseren Produkten von oben bis unten durchgecheckt und haben schließlich das Zertifikat erhalten." Ein Pfund, mit dem er angesichts der Hackerattacken und des riesigen Spionage- und Sabotagepotentials im Netz nun bei seinen Kunden wuchern kann.

[Bildtext:]

Frage: Wo ist hier die Schwachstelle?

Foto Bloomberg

© Alle Rechte vorbehalten. Frankfurter Allgemeine Zeitung GmbH, Frankfurt.

