Informationssicherheit ist eine Unternehmensaufgabe

Die Sicherheit der unternehmenseigenen IT-Infrastruktur wird bei Wirtschaft 4.0 zum wichtigen Faktor. Eine Befragung unter 1.587 Industrieunternehmen und industrienahen Dienstleistern durch 65 Industrie- und Handelskammern ergab im Juni: Die Datensicherheit ist den Unternehmern wichtig oder sehr wichtig für die Wettbewerbsfähigkeit des eigenen Betriebs. Wir sprachen zu dem Thema mit Dr. Sebastian Unger, IT-Sicherheitsbeauftragter der SIV.AG, Roggentin.

Herr Dr. Unger, sind Unternehmen heute schon ausreichend gegen Betriebsstörungen und Anlagenausfälle geschützt?

Schon heute sind viele Unternehmen für das Thema sensibilisiert. Häufig jedoch wird die Einführung eines Prozesses zur Aufrechterhaltung der Informationssicherheit als ressourcenintensive Pflicht wahrgenommen, weil die Aufgabe am Anfang so überwältigend groß erscheint.

Es wird viel über Cyberkriminalität geredet: Was ist besonders gefährdet und warum?

Cyberkriminalität betrifft mittlerweile alle Bereiche unseres Lebens. Einbrüche in schlecht gesicherte Online-Shops machen unsere Privatanschrift und unsere Zahlungsinformation zur Ware für Kriminelle. Moderne Spielzeuge übertragen jedes gesprochene Wort in einem Kinderzimmer zur Auswertung an den Hersteller. Und auch unsere kritischsten Infrastrukturen – Strom, Wasser und Telekommunikation – bieten eine wachsende Angriffsfläche. Die voranschreitende Digitalisierung und Vernetzung gehen einher mit einer steigenden Gefährdung all unserer Lebensbereiche. Wir als Gesellschaft müssen darauf reagieren.

Welche Faktoren sind generell bei der IT-Sicherheit zu beachten?

Bei IT-Sicherheit wird oft an technische Lösungen wie Antiviren-Software und

Dr. Sebastian Unger

Firewalls gedacht. Sie können aber nur dann effektiv eingesetzt werden, wenn ihnen organisatorische Maßnahmen zur Seite gestellt werden. IT und IT-Sicherheit betreffen mittlerweile jeden Mitarbeiter eines Unternehmens. Diese müssen regelmäßig geschult werden.

Systeme werden zunehmend komplexer, werden sie dadurch auch anfälliger?

Das liegt zweifellos in der Natur der Sache. Jüngst wurde bekannt, dass eine verbreitete Malware ihre Befehle von einer Social-Media-Plattform erhielt: Die Kriminellen versteckten die Befehle in scheinbar harmlosen Kommentaren unter Fotos einer bekannten Pop-Sängerin. Für Administratoren des angegriffenen Unternehmens wirkte es, als verbringe ein Mitarbeiter seine Zeit in sozialen Medien. Tatsächlich lud sich die Malware ihre Angriffsbefehle herunter. Die zunehmende Vernetzung einzelner Komponenten zu komplexen, globalen Systemen ermöglicht genau diese gefährlichen Nebeneffekte.

Was ist zu tun?

Informationssicherheit kann nur umfassend funktionieren, wenn sie integraler Bestandteil aller Prozesse eines Unternehmens wird und jeder Mitarbeiter seiner Verantwortung nachkommt. Effektives Informationssicherheits-Management steht und fällt mit einem kontinuierlichen Risiko-Management. Insofern gilt es immer, eine Balance zwischen den Risiken, der Handlungsfähigkeit des Unternehmens und der Wirtschaftlichkeit der erforderlichen Maßnahmen zu finden.

Sie arbeiten mit einem Reifegradmodell als Orientierungshilfe. Welche Kenntnisse gewinnen Unternehmen daraus?

Aus eigener Erfahrung wissen wir, wie überwältigend die Herausforderungen zu Beginn sein können. Das Reifegradmodell dient dabei der eigenen Positionsbestimmung. Hat man sich darin einmal wiedergefunden, so gibt das Modell Handlungsempfehlungen – nicht zuletzt für eine erfolgreiche Zertifizierung.