DIHK Deutscher Industrie- und Handelskammertag

35 Newsletter 30.08.2018

Daten | Fakten | Argumente

THEMA DER WOCHE

Daten- und Informationssicherheit: So entsteht mehr Vertrauen

In den Unternehmen sind zahlreiche IT-Anwendungen im Einsatz, die zunehmend untereinander vernetzt sind – und das nicht nur innerhalb des Unternehmens. Der Vernetzungsgrad mit externen Partnern wie Lieferanten, Kunden oder Behörden steigt, die IT durchdringt alle Unternehmensbereiche, neue Geschäftsmodelle entstehen. Diese Entwicklung bietet Chancen, birgt aber auch ganz neue Bedrohungen. Unternehmen sehen deshalb die Sicherheit ihrer Daten als eine der größten Herausforderungen bei der Digitalisierung an. Was ist zu tun, damit die Daten- und Informationssicherheit nicht zum Hemmschuh der Digitalisierung und damit der künftigen Wettbewerbsfähigkeit der Unternehmen wird?

Gesamtstrategie erforderlich

Der Gesetzgeber ist bereits punktuell tätig geworden: So sind zum Beispiel Mindestsicherheitsstandards und eine Meldepflicht für Sicherheitsvorfälle in besonders kritischen Wirtschaftsbereichen vorgeschrieben. Das reicht aber nicht: Erforderlich ist zudem eine von Politik, Anbietern und Anwendern getragene Gesamtstrategie für ein sicheres „digitales Ökosystem", deren Maßnahmen zielgerichtet ineinandergreifen.

Sicherheit soft- und hardwarebasierter Produkte und Anwendungen verbessern

Zunächst sollten die Anbieter die Vertrauenswürdigkeit von Produkten erhöhen, die auf dem Einsatz von Soft- und Hardware basieren. Das Entwicklungsprinzip „Security by Design" – also die Berücksichtigung von Sicherheitsaspekten in allen Phasen der Softwareentwicklung – sollte obligatorischer Bestandteil der industriellen Standardisierungsprozesse bei Produkten, Softwarekomponenten und anderem sein. Für einen angemessenen Zeitraum sollten die Hersteller Sicherheitsupdates für solche Produkte zur Verfügung stellen. Zur Sensibilisierung der Nutzer kann eine spezielle IT-Sicherheitskennzeichnung beitragen, die mehr Transparenz über die Sicherheitseigenschaften IT-basierter Produkte herstellt. Ein solches Kennzeichen sollte europaweit einheitlich sein.
Der Gesetzgeber sollte nicht zu früh tätig werden. Werden Sicherheitsstandards nicht eingehalten, ist das bestehende Haftungsrecht weitestgehend auf IT-Produkte anwendbar. Daher sind zunächst keine neuen, zusätzlichen Regelungen notwendig. Sinnvoll wäre aber eine Prüfung, inwieweit das bestehende Recht gegenüber Anbietern aus Drittstaaten auch durchgesetzt werden kann.

Finanzielle Unterstützung unbürokratisch anbieten

Die Daten- und Informationssicherheit gehört zur Sorgfaltspflicht eines jeden Geschäftsführers, der IT im Einsatz hat. IHKs und diverse IT-Sicherheitsinitiativen helfen dabei, grundlegende Maßnahmen zu ergreifen. Darüber hinaus bieten Bund und Länder zum Teil auch finanzielle Unterstützung für Beratung, Weiterbildung oder für die Einführung technischer und organisatorischer Maßnahmen. Diese Angebote sollten weiter ausgebaut und einfacher zugänglich gemacht werden.

Mitarbeiter befähigen

Ein wichtiger Faktor für mehr Sicherheit in den Unternehmen sind deren Mitarbeiter. Digitalkompetenzen sind Voraussetzung dafür, dass auch IT-Sicherheit besser verstanden und eingeschätzt werden kann. Digital- und IT-Sicherheitskompetenzen sollten schon in der Schule, in der Ausbildung, im Studium sowie in der beruflichen Weiterbildung auf dem Lehrplan stehen. Erforderlich dafür sind nicht nur finanzielle Mittel für den Anschluss aller Schulen ans schnelle Internet und die Ausstattung der Schulen mit technischen Geräten, sondern auch eine stärkere Gewichtung entsprechender Lerninhalte in der Lehrerausbildung und in IT-Studiengängen.

Reaktionsfähigkeit von Unternehmen und Staat verbessern

Insbesondere kleine und mittlere Unternehmen stehen derzeit noch zu wenig im Austausch mit Sicherheitsbehörden und anderen Betrieben. Deshalb ist es wichtig, das Zusammenspiel zwischen Staat und Wirtschaft effektiver zu organisieren. Unternehmen benötigen sachkundige Ansprechpartner in den Regionen, die es etwa bei IHKs gibt, und kürzere Kommunikationswege mit den Sicherheitsbehörden auf Landesebene. Alle Bundesländer haben inzwischen zentrale Ansprechstellen für Unternehmen eingerichtet. Diese müssen weiter ausgebaut werden – quantitativ und qualitativ.
Die Eckpunkte des DIHK für eine Gesamtstrategie gibt es zum Download unter http://www.dihk.de/it-sicherheit

Ansprechpartnerin: *Dr. Katrin Sobania, DIHK Berlin, Telefon 030 20308-2109*