IT-Sicherheit: „Firmenexistenzen und Arbeitsplätze stehen auf dem Spiel“

Um der wachsenden Bedrohung durch Cyber-Angriffe zu begegnen, hat der Gesetzgeber in den vergangenen Jahren eine Reihe von Gesetzen verabschiedet und zwar nicht nur für Betreiber kritischer Infrastrukturen. Unternehmen sind angehalten, ihre IT-Sicherheitsmaßnahmen regelmäßig zu überprüfen und dem Stand der Technik anzupassen. In einem einstündigen Webinar führte Dr. Anne Förster, Taylor Wessing, Ende September durch eine Expertendiskussion zum Thema.

© Pixabay

Das Bild vom Einzeltäter ist überholt – inzwischen stehen „Fabriken“ hinter Cyber-Angriffen.

Ein ganzer Flickenteppich von Regelungen sei zu beachten, erläuterte Mareike Christine Gehrmann, Fachanwältin für IT-Recht bei Taylor Wessing, und nannte beispielhaft das IT-Sicherheitsgesetz 2.0, Regelungen der EU zur IT-Sicherheit und natürlich die DSGVO, die besonders auf personenbezogene Daten schaue, und deshalb besonders betrachte, wie Schutzmaßnahmen für IT-Systeme zum Schutz von personenbezogenen Daten beitragen können. „Die Automobilindustrie hat sich internationale Standards zur IT-Sicherheit gegeben.“ Vor allem Unternehmen, die international tätig sind, müssten im Rahmen der Produktentwicklung genau schauen, was im jeweiligen Land gilt.

Wolfgang Straßer, Geschäftsführer der @yet-GmbH, nannte drei Haupteinfallstore für Cyber-Kriminelle: Phishing-Attacken, das Ausnutzen von Lücken in den Systemen (Firewalls etc.) und „tatsächlich auch immer noch der berühmte USB-Stick, der irgendwo auf dem Betriebsgelände fallen gelassen und von einem Mitarbeiter in einen PC des Unternehmens gesteckt wird“.

Rolf Fellmann, Geschäftsführer der dSales Plus GmbH, ergänzte: „Wir sollten nicht vergessen, dass eine Lücke im System auch sein kann, das Pendel zu stark ausschlagen zu lassen. Das ist der Fall, wenn Systeme so stark abgesichert werden, dass Menschen nicht mehr arbeiten können und sich dann andere Wege zum Informationsaustausch suchen – z.B. über die private E-Mail-Adresse.“

Straßer wies auf die Schäden hin, die Cyber-Angriffe verursachen: Der Digitalverband Bitkom beziffert den jährlichen Gesamtschaden für die deutsche Wirtschaft 2020/2021 durch Cyber-Angriffe auf 223 Mrd. Euro. Trotz dieser immensen Zahl wüssten viele Unternehmen nicht, wie sie vorgehen sollen, wenn ein Angriff erfolgt. „Das haben viele Unternehmen nicht auf dem Schirm. Dabei sind die ersten Schritte besonders wichtig: Wen sprechen wir an? Was sollte ich keinesfalls tun?“ Straßer beschrieb, dass manche Unternehmen versuchten, dem Schaden durch Löschen zu begegnen. „Das sollten Sie aber auf keinen Fall tun, denn dann sind keine Spuren mehr da, die nachverfolgt werden können.“

Wichtig sei, dass jedes Unternehmen individuell für sich selbst definiere, welche Schritte im Fall eines Angriffs unternommen werden müssten. Zwar gebe es Hilfestellungen und Leitlinien, „die passen aber nie genau auf die Unternehmensstruktur: Welche Kunden muss ich informieren etc. – das ist für jeden unterschiedlich. Das sollte jeder für sich individuell festlegen und dann auch mal geübt haben“.

Gehrmann lenkte den Blick auf kleinere Unternehmen, die zunehmend ins Visier der Behörden gelangen. Denn „jedes Unternehmen ist aufgrund der allgemeinen zivilrechtlichen Regelungen verpflichtet, sich zu schützen und natürlich auch aufgrund der DSGVO. Da gibt es auch abseits kritischer Infrastrukturen viel Potenzial, was es zu schützen gilt.“ Eine weitere Frage könne auch sein, „welche Verpflichtungen mir meine Kunden mitgegeben haben“.

Fellmann appellierte, dass IT-Sicherheit auf die Geschäftsleitungsebene gehöre. „Das ist eine riesige Verantwortung. Die Frage ist ja auch, wer haftet für solche Fälle.“

Förster bekräftigte: „Natürlich ist die Geschäftsführung dazu da, ein Compliance-System zu entwickeln und dazu gehört auch die IT-Security. Die Geschäftsführung ist auch gefordert, die Mitarbeiter verstärkt zu schulen.“

Straßer lenkte den Blick auf die Wertschöpfung, die ohne IT nicht mehr vorstellbar sei. „Auch darum gehört das Thema in die Geschäftsleitung und in das Risikomanagement. International tätige Unternehmen mit angloamerikanischen Investoren geben inzwischen auch entsprechende Goals vor.“

„Nicht zu vergessen ist, dass auch der Reputationsschaden immens ist“, ergänzte Gehrmann.

Zumindest das finanzielle Risiko ließe sich durch eine Cyber-Versicherung mindern. „Allein das, was die Forensiker an Kosten produzieren, ist immens. Jedes Gerät, das in einem Netz ist, das verschlüsselt wurde, muss angepackt und neu aufgesetzt werden. Dazu kommen noch die Ausfallkosten, wenn nicht weiter produziert werden kann.“

Gehrmann erinnerte daran, dass Grundvoraussetzung dafür, überhaupt eine entsprechende Versicherung zu bekommen, aber ein gewisser IT-Security-Standard ist. „Nur die Versicherung ist darum sicher keine Lösung.“

Zum Ende der Runde bat Förster um einen Ausblick auf die kommenden Jahre.

„Wir müssen mehr digitalisieren, um effizienter zu werden. Das erhöht natürlich auch den Aufwand für IT-Security“, sagte Fellmann und forderte viel stärker interdisziplinär an das Thema Cyber-Security heranzugehen: „Bei aller Sicherheit müssen wir in den Unternehmen auch arbeitsfähig bleiben.“

Gehrmann stellte weitere Verschärfungen durch den Gesetzgeber in Aussicht. „Die neue BSI-Kritis-Verordnung hat noch Lücken und setzt noch nicht das IT-Sicherheitsgesetz 2.0 um. Da wird es nochmal eine Anpassung geben. Der Gesetzgeber nimmt das Thema aber auch an diversen anderen Stellen in den Fokus.“

Straßer sieht die maximale Abhängigkeit von der IT auf Unternehmen zukommen. Und damit auch eine rasante Erhöhung der Zahl und der Organisation der Angreifer. „Das sind Fabriken die da angreifen. Darum brauchen wir Awareness top-down – vom Vorstand bis zum Sachbearbeiter muss das gesichert sein.“ Denn am Ende stünden Firmenexistenzen und Arbeitsplätze auf dem Spiel. *chk*