Relevanz von IT-SIcherheit

Nach einer Studie des nordrhein-westfälischen Landesamtes für Verfassungsschutz (LfV) kam es im Jahr 2014 im Durchschnitt alle drei Minuten zu Hacker-Angriffen. Alleine in NRW wurden bereites 370.000 Unternehmen im Jahr 2014 attackiert. Dabei sind Schäden entstanden, die sich auf etwa 50 Mrd. Euro beziffern lassen. Allein Russland und China sollen dabei an 50% aller Angriffe beteiligt gewesen sein. So verwendet der russische Geheimdienst hochprofessionalisierte Technologien, denen im Zweifel nicht einmal die umfangreichen Sicherheitsmaßnahmen von Großkonzernen standhalten können, um Industriespionage zu betreiben. Dass Nachrichtendienste für einen Hauptteil der Wirtschaftsspionage verantwortlich sind, ist sogar im russischen Gesetz vorgeschrieben: demnach soll die Wirtschaft von Geheimdiensten gefördert werden. Während im Jahr 2013 lediglich 27% aller deutschen Unternehmen von Hacking betroffen waren, lag die Zahl 2015 bei ca. 40%. Ein Drittel aller Delikte entfiel auf bargeldlose Zahlungssysteme. Insgesamt waren 55% aller Finanzdienstleister von Angriffen betroffen.

Nicht nur die großen, international agierenden Konzerne sind den Gefährdungen durch Computer- und Cyberkriminalität ausgesetzt. Einer Umfrage der Beratungsgesellschaft PricewaterhouseCoopers (PwC) zufolge, unterschätzen grade die mittelständischen Unternehmen die Problematik. So wurde 2014 durchschnittlich jedes zehnte mittelständische Unternehmen attackiert. Die Schadenssumme lag im Schnitt bei 80.000 Euro. Vereinzelt entstanden wirtschaftliche Schäden in Höhe einer halben Million Euro, im Jahr davor wurde die Schadenssumme bei den meisten Fällen noch auf 10.000 Euro beziffert. Vor allem die Branchen Transport und Logistik, sowie Technologie, Medien und Telekommunikation haben in Sachen Informationssicherheit erheblichen Nachholbedarf. Zur Zeit fehlt es noch an Gefahrenbewusstsein. Durch einen sensibleren Umgang der Geschäftsführung und Mitarbeiter mit Daten, könnte der wirtschaftliche Schaden schon erheblich reduziert werden.

Durch die Angriffe wollen Kriminelle der Konkurrenz entweder Schaden zufügen und/oder sich selbst bereichern. Die Folgen der Hacker-Angriffe lauten: Einnahmeverluste, Datendiebstahl, Know-how-Diebstahl, Produktionsausfälle, Gefährdung von Umwelt, Menschen und Maschinen. Organisierte Täterbanden versuchen vor allem an geistiges Eigentum zu gelangen. Industriespionage verursacht weitaus nachhaltigere Schäden als das Stehlen von Geldbeträgen. Zusätzlich bestehen Reputationsrisiken. Der Begriff Reputation meint das Ansehen beziehungsweise Image eines Unternehmens. Werden Schadensfälle größerer Unternehmen medienwirksam bekannt, verliert der Konzern an Glaubwürdigkeit. Im Jahr 2015 kam es zu einem spektakulären Fall, in welchem Millionen Nutzerdaten von Sony Playstation und einer Partnervermittlung-Agentur an die Öffentlichkeit drangen. Dies führt zu immensen Vertrauensschaden und Verunsicherung bei den Nutzern, was ein Kundenverhältnis verschlechtert oder gar beenden kann. Ein negatives Image ruft eine niedrigere Ertragslage hervor, zudem kommt es zu einer Verschlechterung der Vermögensverhältnisse und zu Wertminderungs-Effekten.

Das Interesse an Informationssicherheit ergibt sich nicht bloß aus Gefahren wie Wirtschaftsspionage, Finanzstraftaten und Marktmanipulation. Darüber hinaus führen Opportunitätskosten und die Beseitigung des Schadens zu erheblichen Kosten.