Cyber-Sicherheit

Staat hinkt hinterher

[02.04.2019] Zwar ist das Thema Cyber-Sicherheit in Deutschland mittlerweile im politischen Diskurs angekommen, bei der Zusammenarbeit zwischen Staat und Cyber-Sicherheitsindustrie passiert aber noch zu wenig.

Anfang Januar wurden im Rahmen eines Hacker-Angriffs private Daten etlicher deutscher Politiker veröffentlicht. Neben Bundeskanzlerin Angela Merkel waren beispielsweise auch Andrea Nahles oder Annegret Kramp-Karrenbauer betroffen. Insgesamt wurden knapp 1.000 Abgeordnete gehackt. Spätestens dieser Vorfall hat die deutsche Politik wachgerüttelt: Cyber-Kriminalität ist eine ernst zu nehmende Bedrohung und es bedarf einer engeren Zusammenarbeit zwischen Regierungsstellen und der Cyber-Sicherheitsindustrie, um den Cyber-Kriminellen einen Schritt voraus sein zu können.
Aktuell gibt es in Deutschland verschiedene kleinere Cyber-Sicherheitsteams, die in Organisationen wie dem BND und der Bundeswehr tätig sind. Allerdings arbeiten diese Teams oft isoliert voneinander und es fehlt an Koordinierung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) übernimmt zwar die zentralisierte Organisation der einzelnen Einrichtungen, aber es gibt noch viel Nachholbedarf. So gestaltet sich auch die Umsetzung des Nationalen Cyber-Abwehrzentrums, das für eine nachhaltige und gesamtstaatliche Cyber-Sicherheitsarchitektur sorgen soll, recht zäh. Grund hierfür ist unter anderem, dass die finanziellen Mittel, die der Staat für die Cyber-Abwehr zur Verfügung hat im Vergleich zu anderen Ländern viel zu gering sind. So werden teilweise auch deutsche Firmen vom Staat beauftragt bei Sicherheitsfragen zu helfen, da die Behörden die Bearbeitung finanziell und personell oft nicht stemmen können.

Gemeinsame Schritte gegen Cyber-Kriminelle

Um mit Cyber-Kriminellen Schritt halten zu können, muss die Zusammenarbeit zwischen Staat und der Cyber-Sicherheitsindustrie Geschwindigkeit aufnehmen. So könnten in einem ersten Schritt Security Operations Center (SOCs), also die Zentralen für alle sicherheitsrelevanten Services im IT-Umfeld von Organisationen oder Institutionen, gemeinsam von Staat und Industrie betrieben werden. Somit wäre ein schnellerer informeller Abgleich bei aktuellen Bedrohungen gewährleistet. Oft haben Experten für bestimmte Nischenthemen in der Cyber-Sicherheit vom Staat außerdem keine offizielle Sicherheitsfreigabe (Clearance) und können deshalb nicht beraten. Der Aufbau eines externen Sicherheitsexperten-Netzwerks außerhalb der Clearance wäre deshalb ein weiterer wichtiger Schritt, da es die Bedrohungsanalyse erheblich verbessern würde.
Damit die Vernetzung von Informationen nicht nur auf Geheimdienstebene, sondern auch im operativen Bereich stattfindet, muss der Staat mehr externe Firmen und Hersteller miteinbeziehen. Denkbar wäre zudem ein regelmäßiger gemeinsamer Cybersecurity Summit von Industrie und Regierung. Nicht zuletzt bedarf es einer Aufstockung von Ressourcen im öffentlichen Haushalt.
Insgesamt müssen Behörden innovativer und agiler werden, wenn es um aktuelle Bedrohungen geht. Dazu gehört beispielsweise auch die Nutzung von aktiven Verteidigungstechnologien – so genannten Response Verfahren – also Technologien, die über die Bedrohungserkennung hinaus arbeiten.

()

Stichwörter: IT-Sicherheit, McAfee