Dennis-Kenji Kipker

Cyber-Sicherheitsstrategie

Cyber-Sicherheitsstrategien sind die politische „Blaupause" für das gesetzgeberische und behördliche Handeln zur Beförderung der Cybersicherheit, die sich regelmäßig als Zusammenarbeit zwischen Behörden und Unternehmen im Sinne einer Public Private Partnership (PPP) darstellt. Schon im Jahr 2005 legte die Bundesregierung den Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) vor, der als nationale IT-Sicherheitsstrategie unter der Leitung des BMI mit fachlicher Unterstützung des BSI erstellt wurde. Hauptanliegen des NPSI war die Reduzierung der durch die vernetzte Datenverarbeitung entstehenden Risiken für die Cybersicherheit. Der NPSI gab seinerzeit drei strategische Ziele innerhalb der Kategorien Prävention, Reaktion und Nachhaltigkeit vor. Hierzu gehörte der angemessene Schutz von Informationsinfrastrukturen, die wirkungsvolle Reaktion auf IT-Sicherheitsvorfälle, sowie die Stärkung der deutschen IT-Sicherheitskompetenz. Auf dem NPSI basierend wurden der Umsetzungsplan für die Bundesverwaltung (UP Bund) und der Umsetzungsplan für die Kritischen Infrastrukturen (UP KRITIS) entwickelt.

2011 wurde der NPSI durch die nationale Cyber-Sicherheitsstrategie der Bundesregierung abgelöst – die aktuelle Fassung der deutschen Cyber-Sicherheitsstrategie stammt aus dem Jahr 2016. Diese baut inhaltlich auf den strategischen Ansätzen und Zielen der ersten Cyber-Sicherheitsstrategie auf, hat diese aber an die neuen Erfordernisse durch die zwischenzeitlich geänderte Bedrohungslage angepasst. Hervorzuheben ist in diesem Zusammenhang, dass Cybersecurity nicht mehr nur als rein nationalstaatliche Aufgabe begriffen werden kann, sondern ein grenzüberschreitendes Vorgehen erfordert, das von der Mikro-, über die Meso-, bis hin zur Makro-Ebene reicht. Dementsprechend untergliedert sich die nationale Cyber-Sicherheitsstrategie aus 2016 in vier Handlungsfelder, die an diese Aufteilung anknüpfen. Im Mittelpunkt des ersten Handlungsfelds „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt" steht der Verbraucherschutz. Hiervon umfasst sind die Förderung der digitalen Kompetenz, die Schaffung von Voraussetzungen für eine sichere elektronische Kommunikation, sichere Webangebote und sichere elektronische Identitäten und die Einführung eines Gütesiegels für IT-Sicherheit – ein Vorschlag, der auch durch den aktuellen Entwurf für ein IT-SiG 2.0 aufgegriffen wird. Das zweite Handlungsfeld der Cyber-Sicherheitsstrategie hat einen weiter gefassten Fokus und stellt die Zusammenarbeit von Staat und Wirtschaft in den Mittelpunkt. Hierzu gehören unter anderem die Absicherung von Kritischen Infrastrukturen, die Stärkung der deutschen IT-Wirtschaft, die Verbesserung der Zusammenarbeit mit Providern und IT-Sicherheitsdienstleistern und die Schaffung einer Plattform für den vertrauensvollen Informationsaustausch. Im dritten Handlungsfeld der aktuellen Cyber-Sicherheitsstrategie wird vornehmlich auf den Staat als Gewährleistungsverantwortlichen für die Cyber-Sicherheit abgestellt. Hierzu zählen die Weiterentwicklung des Nationalen Cyber-Abwehrzentrums (NCAZ), die Stärkung der Fähigkeit zur Analyse und Reaktion vor Ort, die Intensivierung der Strafverfolgung im Cyber-Raum, die Einrichtung eines Frühwarnsystems gegen Cyber-Angriffe aus dem Ausland und die effektive Bekämpfung von Cyber-Spionage und Cyber-Sabotage. Überdies war die Errichtung der mittlerweile bestehenden Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) vorgesehen. Das vierte Handlungsfeld der geltenden nationalen Cyber-Sicherheitsstrategie behandelt die aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik. Dies betrifft nicht lediglich den Ausbau von „Cyber Capacity Building" im Sinne der Förderung bilateraler und regionaler Unterstützungsleistungen zum Auf- und Ausbau von Cyber-Fähigkeiten, sondern auch die Weiterentwicklung der internationalen Cyber-Verteidigungspolitik und die Stärkung der internationalen Strafverfolgung im digitalen Raum.

Jüngst hat das BMI zur Evaluierung und Fortschreibung der 2016er-Strategie aufgerufen. Hierzu fanden im September und Oktober 2020 vier Evaluierungsworkshops statt, die sich thematisch an den vier Handlungsfeldern orientieren. Auch wenn für eine überarbeitete deutsche Cyber-Sicherheitsstrategie im Wesentlichen an den bestehenden inhaltlichen Schwerpunkten festgehalten wird, so wurden diese dennoch an die neuen technischen Entwicklungen und geänderten Bedrohungslagen angepasst. Dies umfasst die Themen digitale Souveränität, Messbarmachung von IT-Sicherheit, Usability, Security by Design, Krisenmanagement, Forschung, Pflichten von IT-Herstellern und Lieferanten, Einbeziehung von Unternehmen, die unterhalb der Schwelle der Kritischen Infrastruktur liegen, Ausbau der Rolle des mit zunehmenden Befugnissen ausgestatteten BSI, und die Förderung eines einheitlichen EU-Regulierungsrahmens mit dem strategischen Ziel einer Vorreiterstellung Deutschlands. Geplant ist die Beschlussfassung über die aktualisierte Cyber-Sicherheitsstrategie gegenwärtig für Mai 2021.