22

Die japanische Cybersicherheitspolitik

Mihoko MATSUBARA

Einleitung

Dieser Beitrag beschäftigt sich mit den Schäden, die in Japan durch Cyberangriffe verursacht wurden, beginnend mit einer Cyberattacke im Jahr 2000, die Auslöser der japanischen Bemühungen um mehr Cybersicherheit war, bis hin zu den aktuellen Bedrohungen im Zusammenhang mit dem russischen Überfall auf die Ukraine im Jahr 2022 und den bis zum Sommer 2023 aufgetretenen Ransomware-Angriffen. Dabei möchte ich untersuchen, welche Art von Politik und internationaler Kooperation Japan angesichts dieser sich verändernden Bedrohungslagen bisher verfolgt hat und was für eine Politik in Zukunft erforderlich sein wird.

Historischer Hintergrund

Ein wichtiger Auslöser für die Bemühungen der japanischen Regierung im Bereich der Cybersicherheit war ein Vorfall im Januar 2000, bei dem die Websites staatlicher und kommunaler Behörden wie der Nationalen Behörde für Wissenschaft und Technik und des Ministeriums für Inneres und Telekommunikation manipuliert worden waren. Mit dem zunehmenden Einsatz von Informationstechnologie (IT) entstand ein dringender Bedarf für Sicherheitsmaßnahmen und Strategien in diesem Bereich, was Ende Februar 2000 zur Einrichtung des „Büros zur Förderung von Informationssicherheitsmaßnahmen des Kabinettssekretariats“ führte (2005 wurde es dann im Rahmen einer Umstrukturierung in *National Information Security Center* umbenannt). Im September 2011 folgten Cyberangriffe auf die Unternehmen Mitsubishi Heavy Industries, IHI und Kawasaki Heavy Industries, wodurch das Interesse am Thema Cybersicherheit in Japan zunehmend wuchs.

Vor diesem Hintergrund wurde Tokyo im September 2013 als Austragungsort für die Olympischen und Paralympischen Sommerspiele 2020 ausgewählt. Die Olympischen Spiele, die weltweite Aufmerksamkeit auf sich ziehen, waren bereits in der Vergangenheit Ziel von Cyberangriffen. Die Sicherheit sowohl im physischen Raum als auch im Cyberspace war für den Erfolg der Olympischen Spiele von entscheidender Bedeutung, weshalb Japan seinen Einsatz zur Stärkung der Cybersicherheit erhöhte. Die japanische Regierung führte daraufhin im November 2014 eine Umstrukturierung ihres Sicherheitszentrums auf Grundlage des Grundgesetzes zur Cybersicherheit durch, indem sie das *National center of Incident readiness and Strategy for Cybersecurity* (NISC) einrichtete. Zu den wichtigsten Aufgaben des NISC gehören die Planung grundlegender Strategien für die japanische Cybersicherheitspolitik und die Zusammenarbeit mit allen Ministerien und Behörden. Außerdem fungiert es als Kontaktstelle für die internationale Zusammenarbeit sowie als öffentlich-private Partnerschaft für den Schutz kritischer Infrastrukturen. Darüber hinaus werden dort die

neuesten Informationen zum Thema Cyberangriffe gesammelt. Weitere zentrale Behörden, die für die Cybersicherheitspolitik zuständig sind, sind das Außenministerium (Cyberdiplomatie), das Verteidigungsministerium (Sicherheit), die Nationale Polizeibehörde (Cyberkriminalität), das Ministerium für Inneres und Telekommunikation (Information und Kommunikation), das Ministerium für Wirtschaft, Handel und Industrie (Gesamtheit der Industrie) und die Digitalbehörde (digitale Transformation).

Da sich ein durch Cyberangriffe verursachter Schaden über die gesamte Lieferkette und damit über Geschäftszweige und Landesgrenzen hinweg verbreiten kann, ist ein Informationsaustausch zur Vorgehensweise bei Cyberangriffen und den diesbezüglichen Maßnahmen sowie eine internationale Kooperation im Bereich der Förderung der Personalentwicklung erforderlich. Japan hat sich im Zusammenhang mit cyberbezogenen Themen unter anderem um bilaterale Verhandlungen mit Israel, Indien, der Ukraine, dem Vereinigten Königreich, Estland, Australien, Deutschland, Frankreich und den USA bemüht und engagiert sich zudem für die multilaterale Zusammenarbeit mit der EU.

Die Gewährleistung eines sicheren Geschäftsumfelds ist auch in Südostasien wichtig, wo viele japanische Unternehmen Niederlassungen gegründet haben und die Zusammenarbeit Japans mit dem Verband Südostasiatischer Nationen (engl. *Association of Southeast Asian Nations*, kurz ASEAN) gefördert wurde. Seit 2009 findet jedes Jahr das *Japan-ASEAN Information Security Policy Meeting* (nun *Japan-ASEAN Cyber Security Policy Meeting* genannt) statt, zu dem Beamte auf Abteilungsleiterebene und Regierungsräte eingeladen werden, um unter anderem über den Schutz kritischer Infrastrukturen zu diskutieren. Im Jahr 2018 gründete das Ministerium für Inneres und Telekommunikation zudem das *ASEAN-Japan Cybersecurity Capacity Building Centre* im thailändischen Bangkok.

Außerdem hat das Gastgeberland Japan auf dem G7-Gipfel in Ise-Shima im Mai 2016 als eines der Ergebnisdokumente die „Grundsätze und Maßnahmen der G7 zum Thema Cybersicherheit" herausgegeben und sich mit allen Teilnehmenden darauf geeinigt, die diesbezügliche Kooperation innerhalb der G7 zu verstärken. Darüber hinaus ist die Zusammenarbeit im Bereich der Cybersicherheit auch Teil des Quadrilateralen Sicherheitsdialogs zwischen Japan, den USA, Australien und Indien (QUAD).

Aktueller Stand und Herausforderungen

Die Olympischen und Paralympischen Spiele 2020 in Tokyo, die inmitten der Coronavirus-Pandemie stattfanden, kamen im September 2021 erfolgreich zum Abschluss. Obwohl die zur Durchführung der Spiele verwendeten

Systeme und Netzwerke ganzen 450 Millionen Cyberangriffen – doppelt so vielen wie bei den Olympischen Spielen 2012 in London – ausgesetzt waren, wurden keine Schäden verursacht, die den Ablauf der Spiele beeinträchtigten. Dies stellt eine großartige Leistung aus Sicht der Cyberabwehr in der Geschichte der Olympischen Spiele dar. Assistenzprofessor Brian Gantt von der Maryville University in den USA, der schwerpunktmäßig zu Cybersicherheit forscht, lobte die Cybersicherheitsmaßnahmen im Rahmen der Tokyo-Olympiade 2020 in den höchsten Tönen und bezeichnete sie als ein vorbildliches Beispiel, dem alle Organisationen von Veranstaltungen folgen sollten.

Vor dem Hintergrund der Lieferkettenprobleme während der Pandemie verabschiedete Japan im Mai 2022 außerdem ein Gesetz zur Förderung der wirtschaftlichen Sicherheit. Kein Aspekt dieses Gesetzes – weder die Sicherstellung einer stabilen Versorgung mit essenziellen Gütern, die stabile Bereitstellung kritischer Infrastrukturleistungen noch die Unterstützung der Entwicklung fortschrittlicher Schlüsseltechnologien – lässt sich ohne Cybersicherheit verwirklichen, weshalb dieses Gesetz zu deren Stärkung von essenzieller Bedeutung ist.

Darüber hinaus hat die japanische Regierung in ihrer im September 2021 veröffentlichten Cybersicherheitsstrategie „drastische Maßnahmen zur Erhöhung der Abschreckungskraft gegenüber Cyberangriffen“ beschlossen, und zwar unter Einsatz „aller verfügbaren politischen, wirtschaftlichen, technischen, rechtlichen, diplomatischen und sonstigen Mittel und Fähigkeiten“. Diese Formel lässt sich als Vorreiterin des Konzepts der „aktiven Cyberabwehr“ betrachten, das durch seine Integration in die „Nationale Sicherheitsstrategie“ vom Dezember 2022 für Aufmerksamkeit sorgte. Diese aktive Cyberabwehr ermöglicht es der japanischen Regierung, darunter dem Verteidigungsministerium und den Selbstverteidigungsstreitkräften, Maßnahmen zur rechtzeitigen Beseitigung einer Bedrohung durch Cyberangriffe und zur Verhinderung einer Ausbreitung von Schäden zu ergreifen, wenn „die Gefahr eines ernsthaften Cyberangriffs besteht, der Sicherheitsbedenken für den Staat und kritische Infrastrukturen usw. zur Folge haben könnte“ – auch wenn ein solcher Angriff die Schwelle eines bewaffneten Angriffs nicht überschreitet.

Denn auch Cyberangriffe, die die Schwelle eines bewaffneten Angriffs nicht überschreiten, können erheblichen Schaden anrichten. Der Ransomware-Angriff auf die Colonial Pipeline in den USA im Mai 2021 bewies, dass ein solcher Schaden sich selbst dann auf die gesamte Lieferkette ausweiten und zu einer nationalen Sicherheitskrise führen kann, wenn nur ein einziges Unternehmen innerhalb der kritischen Infrastruktur zum Opfer von Cyberkriminalität wird, die finanziell motiviert ist. Auch in Japan unterbrach

ein Ransomware-Angriff auf den Hafen von Nagoya im Juli 2023 die Be- und Entladevorgänge für etwa zwei Tage und hatte erhebliche Auswirkungen auf den Betrieb in der Automobil- und Bekleidungsindustrie zur Folge. Deshalb ist es umso wichtiger, eine „aktive Cyberabwehr" zu realisieren und sicherzustellen, dass der öffentliche und private Sektor zum Schutz kritischer Infrastrukturen miteinander kooperieren.

Zum Abschluss

Nach dem russischen Überfall auf die Ukraine, der im Februar 2022 begann, kommt es auch weiterhin zu gezielten Cyberangriffen gegenüber der Ukraine. Während der Krieg sich weiter hinzieht, müssen Länder, die die Ukraine unterstützen – darunter auch Japan – darauf achten, dass ihre militärischen und humanitären Hilfen für die Ukraine nicht durch solche Cyberangriffe beeinträchtigt werden.

Weder die Wirtschaft noch der Sicherheitssektor können heutzutage ohne IT existieren – daher stellt Cybersicherheit einen zentralen Eckpfeiler der wirtschaftlichen und nationalen Sicherheit dar. Darüber hinaus sind auch öffentlich-private Partnerschaften auf nationaler und internationaler Ebene unerlässlich, da sich Schäden von Cyberangriffen über Lieferketten grenzüberschreitend ausbreiten können. Gerade in der jetzigen Zeit muss Japan all seine Kräfte bündeln und sich darum bemühen, kritische Infrastrukturen zu schützen und seinen Informationsaustausch zu erweitern.

Literaturangaben

Brian Gant (2021), "The Tokyo Olympics are a cybersecurity success story," *Security Magazine*, https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

Microsoft Threat Intelligence (2022), "New "Prestige" ransomware impacts organizations in Ukraine and Poland," https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Tonya Riley (2022), "Iranian hackers planned attack on Boston Children's Hospital last summer, FBI director says," *CyberScoop*, https://cyberscoop.com/iran-hospital-wray-fbi-boston-children/

Mihoko MATSUBARA

Mihoko Matsubara ist Chef-Cybersicherheitsstrategin bei der NTT Corporation in Tokio und verantwortlich für die Führung im Bereich Cybersicherheit. Sie war im japanischen Verteidigungsministerium tätig, bevor sie an der Johns Hopkins School of Advanced International Studies im Rahmen eines Fulbright-Stipendiums ihren Masterabschluss machte. Bevor sie zu NTT kam, arbeitete sie als Vice President und Public Sector Chief Security Officer für den asiatisch-pazifischen Raum bei Palo Alto Networks. Von 2014 bis 2018 war sie Mitglied des Ausschusses für Forschung und Entwicklung im Bereich der Cybersicherheit der japanischen Regierung.

Sie ist Adjunct Fellow am Pacific Forum, Honolulu, und Associate Fellow für Cyber am International Institute for Strategic Studies, London. Im Jahr 2019 veröffentlichte sie ein Buch über Cybersicherheit auf Japanisch bei Shinchosha Publishing Co. Ltd. und wurde dafür von der Okawa Foundation for Information and Telecommunications für 2020 ausgezeichnet.

Sie leistete außerdem einen Beitrag zu „Japans 5G-Sicherheitsstrategie und Wettbewerb in aufstrebenden Technologien“ für das Projekt „Strategisches Japan“ (Wettbewerb in neuen Bereichen) am Japan-Lehrstuhl des Center for Strategic and International Studies im Jahr 2022. Ihr zweites Buch, *Ukraine's Cyber War*, wurde im August 2023 von Shinchosha veröffentlicht und 2024 vom Digital Policy Forum ausgezeichnet.