Ein Überblick über das Cybersicherheitsrecht in Taiwan

von John EASTWOOD, Nathan SNYDER, Wendy CHU, Svea MATTHIESSEN, Lloyd G. ROBERTS III

1. MAßGEBLICHE VORSCHRIFTEN

In Taiwan gibt es in Bezug auf die Informationssicherheit zwei Hauptbereiche der Gesetzgebung: Gesetzgebung zur Cybersicherheit und Gesetzgebung zum Schutz persönlicher Daten. Während die Informationssicherheitsaspekte der Gesetzgebung zum Schutz personenbezogener Daten (hauptsächlich die PDPA) nur für die Sammlung, Speicherung und Verarbeitung personenbezogener Daten gelten, sind die Anforderungen der Gesetzgebung zur Cybersicherheit (hauptsächlich der CSMA) abhängig vom Status der juristischen Person, die die Daten kontrolliert, anwendbar. Bestimmte sektorspezifische Vorschriften gelten umfassender, wie z.B. die Regelungen für den Finanzsektor.

1.1. GESETZGEBUNG

Allgemeine Gesetzgebung

- Der Cyber Security Management Act (CSMA), der im Juni 2018 beschlossen wurde, ist das Kernstück der Gesetzgebung zur Cybersicherheit in Taiwan. Er wird durch die folgenden Regeln und Bestimmungen, die am 1. Januar 2019 in Kraft getreten sind, weiter spezifiziert:
    - Enforcement Rules of the Cybersecurity Management Act (CSMA Durchsetzungsregeln)
    - Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency (Prüfungsbestimmungen)
    - Regulations on the Notification and Response of Cyber Security Incident (Vorschriften für Zwischenfälle)
    - Cyber Security Information Sharing Regulations
    - Regulations on Classification of Cyber Security Responsibility Levels (Klassifizierungsvorschriften)
- Der Personal Data Protection Act (PDPA), zuletzt geändert im Dezember 2015, enthält Bestimmungen zur Informationssicherheit in Bezug auf personenbezogene Daten. Solche Daten dürfen nur dann erhoben, verarbeitet oder genutzt werden, wenn "angemessene Sicherheitsmaßnahmen" getroffen wurden, um die Sicherheit der Daten zu gewährleisten. Die Enforcement Rules of the PDPA (Durchsetzungsregeln) bieten wertvolle Leitlinien für die Auslegung und wurden im März 2016 verabschiedet.
- Criminal Code (Strafgesetzbuch);
- The Communication Security and Surveillance Act (Gesetz über Kommunikationssicherheit und -überwachung);
- National Security Act (Gesetz über die nationale Sicherheit);
- Money Laundering Control Act (Gesetz zur Bekämpfung der Geldwäsche);
- Counter-Terrorism Financing Act (Gesetz über die Bekämpfung der Terrorismusfinanzierung).

Sektorspezifische Gesetzgebung

- The Banking Act of The Republic of China (Bankengesetz)
- Act Governing Issuance of Electronic Stored Value Cards (Gesetz zur Regelung der Ausgabe von elektronischen Wertkarten)
- Rules Governing the Administration of Electronic Payment Business (Regeln für die Verwaltung des elektronischen Zahlungsverkehrs)
- Regulations Governing the Clearinghouse's Plan of Security Measures for Personal Information Files (Vorschriften über den Leitfaden der Clearingstelle für Sicherheitsmaßnahmen für Dateien mit persönlichen Daten)
- Regulations Governing Approval and Administration of Financial Information Service Enterprises Engaging in Interbank Funds Transfer and Settlement (Vorschriften für die Genehmigung und Verwaltung von Finanzdienstleistern, die sich mit Interbankgeldtransfers und -abrechnungen befassen)

- Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (Vorschriften über interne Betriebssysteme und Verfahren für die Auslagerung des Betriebs von Finanzinstituten)
- Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (Durchführungsbestimmungen für die Interne Revision und das Interne Kontrollsystem von Finanzholdinggesellschaften und Bankwesen)
- Regulations Governing Online Insurance Business and Online Insurance Services of Insurance Agent Companies and Insurance Broker Companies (Vorschriften für das Online-Versicherungsgeschäft und die Online-Versicherungsdienste von Versicherungsagenten- und Versicherungsmaklergesellschaften)
- Regulations for Administration of Mobile Broadband Businesses (Vorschriften für die Verwaltung von Mobilfunk-Breitbandgeschäften)
- Regulation Governing Export and Import of Strategic High-Tech Commodities (Vorschrift zur Regelung des Exports und Imports von strategischen High-Tech-Gütern)
- Regulations on Tourist Hotel Enterprise Plans for Maintaining the Security of Personal Information Files (Vorschriften zu den Regelungen der Touristenhotels zur Aufrechterhaltung der Sicherheit von Dateien mit persönlichen Daten)
- Regulations Governing Personal Information File Security Maintenance Plan and Processing Method for the Human Resources Recruitment Industry (Vorschriften für die Sicherheit von Dateien mit persönlichen Informationen, Wartungsplan und Verarbeitungsmethode für die Personalvermittlungsindustrie)
- Regulations Governing Security Protection Plans for and Processing of Personal Information Files by Travel Agencies (Vorschriften über Sicherheitsschutzpläne für die Verarbeitung von Dateien mit persönlichen Daten durch Reisebüros

1.2. AUFSICHTSBEHÖRDEN

- The Financial Supervisory Commission ("FSC") (Finanzaufsichtskommission)
- The National Communications Commission ("NCC") (Nationale Kommunikationskommission)
- National Security Bureau (Büro für Nationale Sicherheit)
- Ministry of Interior (Innenministerium)
- Ministry of Foreign Affairs (Außenministerium)
- Ministry of National Defense (Verteidigungsministerium)
- Ministry of Economic Affairs (Wirtschaftsministerium)
- Central Bank (Zentralbank)
- Andere Regulierungsbehörden, die für bestimmte Industriebereiche zuständig sind

1.3. RICHTLINIEN DER AUFSICHTSBEHÖRDEN

- Zu den allgemeinen Richtlinien im Rahmen des CSMA gehören die
    - Regulations for Classification of Cybersecurity Responsibility (Vorschriften für die Einstufung der Verantwortlichkeiten im Bereich der Cybersicherheit)
    - Regulations for Reporting and Responding Cybersecurity Incidents (Vorschriften für die Meldung und Reaktion auf Vorfälle im Bereich der Cybersicherheit)

    - Regulations for Inspecting Implementation Status of Specific Non-Governmental Agencies' Cybersecurity Maintenance Programs (Vorschriften für die Überprüfung des Implementierungsstatus der Cybersicherheits-Instandhaltungsprogramme bestimmter Nichtregierungsstellen)
    - Cybersecurity Information Sharing Regulations (Vorschriften für den Informationsaustausch im Bereich der Cybersicherheit)
- Laut CSMA haben auch viele spezifische Aufsichtsbehörden der jeweiligen Wirtschaftszweige ihre eigenen Richtlinien für das Cybersicherheitsmanagement herausgegeben

2. ANWENDUNGSBEREICH

Cyber Security Management Act

Der CSMA regelt die Anforderungen an die Cybersicherheit für Regierungsbehörden, mit Ausnahme von Militär- und Geheimdienstbehörden und so genannten "spezifischen Nichtregierungsstellen". Diese nichtstaatlichen Stellen sind Anbieter kritischer Infrastrukturen, staatseigene Unternehmen und von der Regierung aufgesetzte Stiftungen. Darüber hinaus legt der CSMA Anforderungen für das Outsourcing fest. Als solcher gilt der CSMA nicht für Auftragnehmer (oder Unterauftragnehmer) des Militärs oder des Geheimdienstes, es sei denn, diese Auftragnehmer werden selbst als spezifische Nichtregierungsstellen eingestuft.

Die vom CSMA auferlegten Pflichten folgen einem dreistufigen Ansatz:

1. Umsetzung eines Plans zur Aufrechterhaltung der Cybersicherheit, einschließlich der jährlichen Berichterstattung darüber
2. Jährliche Prüfungen der Umsetzung des Plans zur Aufrechterhaltung der Computer- und Netzsicherheit, einschließlich Verbesserungsanforderungen im Falle einer unzureichenden Umsetzung
3. Behandlung und Meldung von Vorfällen im Zusammenhang mit der Cybersicherheit

In Bezug auf private Akteure gilt der CSMA nur für Anbieter kritischer Infrastrukturen (und Parteien, an die der Aufbau oder die Wartung von Cybersicherheitssystemen ausgelagert wurde oder die Cybersicherheitsdienste für Stellen erbringen, die dem CSMA unterstehen). Anbieter kritischer Infrastrukturen sind Akteure, die "kritische Infrastrukturen ganz oder teilweise unterhalten oder bereitstellen, wie von der für die jeweilige Branche zuständigen Zentralbehörde bestimmt". Kritische Infrastruktur wird in Artikel 3.7 des CSMA definiert als "ein Wirtschaftsgut, ein System oder ein Netzwerk, sei es physisch oder virtuell, das, sobald es nicht mehr in Betrieb ist oder an Wirksamkeit verliert, zu erheblichen negativen Auswirkungen auf die nationale Sicherheit, die öffentlichen Interessen, den Lebensstandard der Bürger und die wirtschaftlichen Aktivitäten führen würde".

Bisher wurden bei der Ausarbeitung des CSMA die folgenden Infrastrukturbereiche als kritisch erachtet:

- Energie
- Wasserressourcen
- Kommunikation
- Transport
- Finanzen
- Medizinische Notfallversorgung
- Zentrale und lokale Regierungsstellen
- Wissenschaftszentren

2.1. NETZWERK- UND INFORMATIONSSYSTEME

Cyber Security Management Act

Der CSMA definiert in Artikel 3.1 Informations- und Kommunikationssysteme und -dienste als Systeme oder Dienste, "die dazu verwendet werden, Informationen zu sammeln, zu kontrollieren, zu übertragen, zu speichern, zu verbreiten, zu löschen oder auf andere Weise zu verarbeiten, zu nutzen und zu teilen".

2.2. BETREIBER KRITISCHER INFORMATIONS- INFRASTRUKTUREN

Cyber Security Management Act

Die Kommunikationsinfrastruktur wurde als kritisch eingestuft. Daher gilt der CSMA für diese Betreiber, soweit sie von den zuständigen Behörden als Anbieter kritischer Infrastrukturen ausgewiesen wurden.

Darüber hinaus können der CSMA und damit zusammenhängende Vorschriften indirekt auch auf Betreiber kritischer Informationsinfrastrukturen Anwendung finden, wenn sie ausgelagerte Dienstleistungen für Regierungsbehörden oder bestimmte Nichtregierungsstellen erbringen.

2.3. BETREIBER ESSENTIELLER DIENSTLEISTUNGEN

Cyber Security Management Act

Die Infrastruktur in den Bereichen Energie, Wasser, Transport und medizinische Notfallversorgung wurde als kritisch eingestuft. Daher gilt der CSMA für diese Betreiber, soweit sie von den zuständigen Behörden als Anbieter kritischer Infrastrukturen benannt wurden.

2.4. CLOUD-COMPUTING-DIENSTE

Cyber Security Management Act

Die Kommunikationsinfrastruktur wurde als kritisch eingestuft. Daher gilt der CSMA für diese Dienstleister, soweit sie von den zuständigen Behörden als Anbieter kritischer Infrastrukturen benannt wurden.

Darüber hinaus können der CSMA und die damit zusammenhängenden Vorschriften indirekt auch auf Anbieter von Cloud Computing-Diensten Anwendung finden, wenn sie ausgelagerte Dienste für Regierungsstellen oder bestimmte Nichtregierungsstellen erbringen.

Auch die Nutzung von Cloud-Diensten und der grenzüberschreitende Datentransfer sind im Zusammenhang mit Finanzinstitutionen speziell geregelt. Kundendaten von Finanzinstituten müssen durch Sicherungskopien lokal in Taiwan gespeichert werden.

2.5. ANBIETER DIGITALER DIENSTE

Cyber Security Management Act

Die Kommunikationsinfrastruktur wurde als kritisch eingestuft. Daher gilt der CSMA für diese Betreiber, soweit sie von den zuständigen Behörden als Anbieter kritischer Infrastrukturen bestimmt wurden.

Darüber hinaus können der CSMA und die damit zusammenhängenden Vorschriften indirekt auch auf Anbieter digitaler Dienste Anwendung finden, wenn diese ausgelagerte Dienste für Regierungsstellen oder bestimmte Nichtregierungsstellen erbringen.

2.6. SONSTIGES

Outsourcing unter CSMA

Gemäß Artikel 9 des CSMA kann eine dem CSMA unterstellte Stelle die Einrichtung oder Wartung des Informations- oder Kommunikationssystems oder die Bereitstellung von Informations- oder Kommunikationsdiensten outsourcen. Bei der Auslagerung bleibt die Stelle für die Beaufsichtigung der erbrachten Dienstleistungen zur Aufrechterhaltung der Cybersicherheit verantwortlich und damit auch für die Einhaltung der von dem CSMA und damit zusammenhängenden Vorschriften vorgesehenen Verpflichtungen. Artikel 4 der CSMA Enforcement Rules legt Auswahlkriterien und Auslagerungsanforderungen fest. Dienstleistungsanbieter müssen nachweisen, dass sie Maßnahmen zum Cybersicherheitsmanagement umgesetzt haben und dass sie über qualifiziertes Cybersicherheitspersonal verfügen. Darüber hinaus müssen in Fällen, die Informationen zur

nationalen Sicherheit betreffen, sicherheitsrelevante Hintergrundprüfungen durchgeführt werden, individuelle Entwicklungen müssen sicherheitsüberprüft werden, und der Dienstleister ist verpflichtet, die outsourcende Stelle über jeden Vorfall im Bereich der Cybersicherheit zu informieren, von dem er Kenntnis erhält. Die outsourcende Stelle muss darüber hinaus in der Lage sein, den Service Provider hinsichtlich des Implementierungsstatus seiner Cybersicherheitsmaßnahmen zu überprüfen.

3. VORAUSSETZUNGEN

3.1. SICHERHEITSMAßNAHMEN

A. Cyber Security Management Act

Artikel 16 des CSMA verpflichtet Anbieter kritischer Infrastrukturen, die Anforderungen der Verantwortungsebene für die Cybersicherheit zu erfüllen, wie in den Regulations on Classification of Cyber Security Responsibility Levels und ihren zehn Anhängen festgelegt. Diese Vorschriften sehen fünf Verantwortungsebenen für die Cybersicherheit vor, A bis E, mit zunehmenden Sicherheitsmaßnahmen, die umgesetzt werden müssen, um die Verantwortlichkeiten zu erfüllen. Die Verantwortungsebene eines Anbieters kritischer Infrastrukturen für die Cybersicherheit wird auf der Grundlage der Größe, des Bereichs und der Substituierbarkeit seiner Tätigkeiten sowie der möglichen Auswirkungen im Falle von Störungen festgelegt (Artikel 4 bis 10 der Klassifizierungsbestimmungen).

Je nach Verantwortlichkeitsebene müssen die Anbieter durch die Bereiche Geschäftsleitung, Technologie, Sensibilisierung und Schulung unterschiedliche Kontrollmechanismen einführen. Zu den Kontrollmaßnahmen können die Umsetzung international anerkannter Standards wie CNS 27001 oder ISO 27001, die Beschäftigung von speziellem Cybersicherheitspersonal, die Durchführung halbjährlicher interner Cybersicherheitsaudits, die Beschränkung der Verwendung bestimmter Produkte von Drittanbietern, regelmäßige Tests der Kernsysteme, die Installation von Software und Mechanismen zur Schutz der Cybersicherheit und die Gewährleistung des Bewusstseins für die Cybersicherheit beim gesamten Informationspersonal gehören (Anhänge 1 - 8 der Klassifizierungsvorschriften).

Unabhängig von der Verantwortlichkeitsstufe für die Cybersicherheit muss die Cyber-System-Verteidigungsstufe des Anbieters - hoch, mittel oder allgemein - den höchsten Anforderungen in Bezug auf mindestens eines der Kriterien Vertraulichkeit, Integrität, Verfügbarkeit oder Einhaltung gesetzlicher Vorschriften des Anbieters entsprechen (Anhang 9 der Klassifizierungsvorschriften). Auf der Grundlage dieser Verteidigungsstufe kann ein Anbieter die Mindestanforderungen für sein Cyber-System unter anderem in Bezug auf Zugangskontrolle, Geschäftskontinuität, Benutzeridentifikation und -authentifizierung sowie System- und Informationsintegrität festlegen (Anhang 10 der Klassifikationsvorschriften). Je nach Branche kann es zusätzliche oder andere Verteidigungsstandards für Cybersysteme geben, die von der für diese Branche zuständigen Zentralbehörde erlassen wurden.

B. Personal Data Protection Act

Der PDPA legt keinen spezifischen Sicherheitsstandard für die Wahrung der Vertraulichkeit persönlicher Daten und den Schutz der Privatsphäre fest. Die Enforcement Rules des PDPA bieten jedoch mehr Klarheit über die Art der Mechanismen, die Einrichtungen, die mit personenbezogenen Daten umgehen, anwenden dürfen. Darüber hinaus wurden branchenspezifische Richtlinien für mehrere Wirtschaftsbereiche herausgegeben, die je nach Art der Geschäftstätigkeit strengere Standards vorsehen (z.B. Finanzindustrie, Reise- und Tourismus, Telekommunikation und Personalagenturen).

Artikel 12 der Enforcement Rules des PDPA listet 11 Faktoren auf, anhand derer beurteilt werden kann, ob die von einem Erheber oder Verarbeiter personenbezogener Daten ergriffenen Sicherheitsmaßnahmen angemessen sind. Diese sind:

1. Zuweisung von Managementpersonal und angemessenen Ressourcen;
2. Festlegung des Umfangs der personenbezogenen Daten;
3. Einrichtung eines Mechanismus zur Risikobewertung und Verwaltung persönlicher Daten;
4. Einrichtung eines Mechanismus zur Verhinderung, Benachrichtigung über und Reaktion auf eine Datenverletzung;
5. Einrichtung eines internen Kontrollverfahrens für die Sammlung, Verarbeitung und Verwendung persönlicher Daten;
6. Verwaltung von Datensicherheit und Personal;
7. Förderung der Sensibilisierung, Ausbildung und Schulung;
8. Verwaltung der Betriebssicherheit;
9. Einrichtung eines Audit-Mechanismus für die Datensicherheit;
10. Aufbewahrung von Aufzeichnungen, Protokolldateien und relevanten Beweisen; und
11. Implementierung integrierter und anhaltender Verbesserungen bei der Sicherheit und Verwaltung persönlicher Daten.

3.2. MELDUNG VON CYBERSICHERHEITSVORFÄLLEN

A. Cyber Security Management Act

Artikel 18 des CSMA erlegt den Anbietern kritischer Infrastrukturen im Falle eines Vorfalls im Bereich der Cybersicherheit die Pflicht auf, die Regulierungsbehörden innerhalb einer Stunde nach Bekanntwerden des Vorfalls zu benachrichtigen (wie in Artikel 11 der Incident Regulations näher ausgeführt). Ein solcher Vorfall wird allgemein als ein Ereignis verstanden, bei dem der Zustand des Systems, des Dienstes oder des Netzes wahrscheinlich auf eine Verletzung der Cybersicherheitspolitik oder ein Versagen der Sicherheitsmaßnahmen hindeutet, was sich nachteilig auf das Informations- und Kommunikationssystem auswirkt und somit eine Bedrohung der Cybersicherheit darstellt. Die Meldung muss Einzelheiten wie den Zeitpunkt des Auftretens, eine Beschreibung der Situation, Maßnahmen zur Reaktion auf den Vorfall sowie eine Bewertung des Ausmaßes des Vorfalls enthalten. Gemäß den Regulations on the Notification and Response of Cyber Security Incident gibt es vier

Ebenen von Vorfällen, die im Falle eines Ereignisses zu unterschiedlichen Verantwortlichkeiten führen. Diese Ebenen werden auf der Grundlage des von dem Vorfall betroffenen Unternehmens, der Schwere des Vorfalls und seiner potenziellen Auswirkungen, insbesondere auf kritische Infrastrukturen, festgelegt (Artikel 2 der Incident Regulations).

Nach Bekanntwerden des Vorfalls muss der Anbieter die Schadenskontrolle oder -behebung je nach Vorfallstufe innerhalb von 36 oder 72 Stunden abschließen. Nach Abschluss muss der Anbieter den Vorfall weiter untersuchen und managen und der für die betreffende Branche zuständigen Zentralbehörde einen entsprechenden Bericht vorlegen, der auch die als Reaktion auf den Vorfall ergriffenen Verbesserungsmaßnahmen enthält (Artikel 13 der Incident Regulations). Dieser Untersuchungs-, Management- und Verbesserungsbericht muss innerhalb eines Monats vorgelegt werden und Einzelheiten wie den zeitlichen Rahmen des Ereignisses, eine Schadensbeurteilung, eine Ursachenanalyse des Vorfalls sowie Einzelheiten zu den Maßnahmen enthalten, die ergriffen wurden, um eine Wiederholung ähnlicher Vorfälle zu verhindern (Artikel 8 der CSMA Enforcement Rules).

B. Personal Data Protection Act

Im Rahmen des PDPA besteht keine Verpflichtung zur Benachrichtigung der Regulierungsbehörden im Falle von Verletzungen des Schutzes personenbezogener Daten, die in Artikel 12 definiert sind als jedes Mal, wenn "personenbezogene Daten gestohlen, offengelegt, geändert oder anderweitig aufgrund einer Verletzung des PDPA verletzt werden". Allerdings muss ein Verantwortlicher für personenbezogene Daten die betroffenen Rechtssubjekte benachrichtigen, "nachdem die relevanten Fakten geklärt sind". Eine ausreichende Benachrichtigung muss "die Tatsachen im Zusammenhang mit der Datenverletzung und die bereits getroffenen Maßnahmen zur Bekämpfung dieser Verletzung" enthalten (Artikel 22 der PDPA Enforcement Rules).

3.3. REGISTRIERUNG BEI DER AUFSICHTSBEHÖRDE

Private Akteure, die direkt dem CSMA unterstehen, d.h. Anbieter kritischer Infrastrukturen, werden von der für die jeweilige Branche zuständigen Zentralbehörde benannt. Als solche sind sie nicht verpflichtet, sich bei der Aufsichtsbehörde zu registrieren. Sie haben jedoch das Recht, in der Angelegenheit gehört zu werden, bevor die Benennung formalisiert wird (Artikel 9 der CSMA Enforcement Rules).

3.4. ERNENNUNG EINES SICHERHEITSBEAUFTRAGTEN

A. Cyber Security Management Act

Nur Regierungsbehörden sind verpflichtet, einen Cybersicherheitsbeauftragten zu benennen; für Unternehmen besteht nach dem CSMA keine Verpflichtung dazu. Je nach Verantwortlichkeitsstufe im Bereich der Cybersicherheit kann ein Anbieter kritischer Infrastrukturen jedoch gesetzlich verpflichtet sein, spezialisierte Cybersicherheitsmitarbeiter mit einschlägigen beruflichen Zertifizierungen oder Geschäftserfahrungen zu beschäftigen.

B. Personal Data Protection Act

In ähnlicher Weise sind nach dem PDPA nur Regierungsbehörden ausdrücklich verpflichtet, Datenschutzbeauftragte zu ernennen (Artikel 18). Nach den Enforcement Rules des PDPA ist jedoch die Ernennung von Managementpersonal einer der empfohlenen Faktoren in einem angemessenen System zum Schutz der Privatsphäre. Darüber hinaus können branchenspezifische Vorschriften die Beschäftigung von Fachpersonal erfordern, um den Registrierungs- oder Berichterstattungsanforderungen zu entsprechen.

3.5. Sonstiges

Cybersecurity Maintenance Plan

Gemäß Artikel 16 des CSMA sind Anbieter kritischer Infrastrukturen verpflichtet, einen Plan zur Aufrechterhaltung der Cybersicherheit (Cybersecurity Maintenance Plan) umzusetzen, der unter anderem Punkte wie die auf die Cybersicherheit bezogenen Richtlinien und Mechanismen des Anbieters, die Identifizierung von Kerngeschäften, die Bestandsaufnahme von Informationen und Systemen, breit angelegte Risikobewertungen und Maßnahmen zum Management ausgelagerter Systeme und Dienstleistungen umfasst (Artikel 6 der CSMA Enforcement Rules). Dieser Cybersecurity Maintenance Plan bildet die Grundlage für die Erfüllung der Verpflichtungen des Anbieters im Bereich der Cybersicherheit und dient auch als Grundlage für die Kontrolle der Behörden durch den Auditprozess. Darüber hinaus müssen Anbieter kritischer Infrastrukturen jährlich über den Stand der Umsetzung ihres Plans berichten.

Anbieter kritischer Infrastrukturen sind verpflichtet, bei jährlichen Audits über die Umsetzung ihrer Pläne zur Aufrechterhaltung der Cybersicherheit zu kooperieren. Diese Audits werden fest terminiert und können nur einmal durch schriftliche Mitteilung innerhalb von fünf Tagen nach Erhalt der Mitteilung über das Auditprogramm verschoben werden, außer in Fällen höherer Gewalt (Artikel 4 der Audit Regulations). Während eines solchen Audits überprüft die zuständige Behörde den Stand der Umsetzung des Cybersecurity Maintenance Plans und kann vom Auditierten verlangen, beim Vorauditgespräch und beim physischen Vor-Ort-Audit zu kooperieren sowie Erklärungen, relevante Dokumente und unterstützende Informationen zu liefern (Artikel 5 der Audit Regulations).

Wenn die Ergebnisse des Audits Unzulänglichkeiten oder Mängel bei der Umsetzung des Cybersecurity Maintenance Plans aufzeigen, muss der Anbieter kritischer Infrastrukturen innerhalb eines Monats nach Erhalt der Ergebnisse des Audits einen Verbesserungsbericht vorlegen (Artikel 8 der Audit Regulations). Dieser Verbesserungsbericht muss die Mängel oder die zu verbessernden Punkte, die Ursachen des Auftretens, spezifische Verbesserungsmaßnahmen, die ergriffen werden sollen, den geschätzten Zeitplan für diese Maßnahmen sowie Mechanismen zur Verfolgung des Umsetzungsfortschritts enthalten (Artikel 3 der CSMA Enforcement Rules).

Übungen zur Cybersicherheit

Ähnlich zu den Audits müssen Anbieter kritischer Infrastrukturen auch Cybersicherheitsübungen durchführen, wie z.B. Angriffs- und Verteidigungsübungen oder Szenarioübungen (Artikel 19 der Incident Regulations). Dies steht im Zusammenhang mit der alle zwei Jahre stattfindenden Prüfung von Systemeindringungen, die von bestimmten Nichtregierungsstellen durchgeführt werden müssen, die für die Cybersicherheit der Stufen A, B oder C zuständig sind (Classification Regulation, Anhänge 2, 4 und 6). Die Cybersicherheitsübungen sind jedoch für alle kritischen Infrastrukturen erforderlich, unabhängig von ihrem Verantwortungsgrad im Bereich der Cybersicherheit.

Mobile Breitbandbetreiber sind gemäß den Regulations for Administration of Mobile Broadband Businesses (Artikel 83-1) verpflichtet, Eindringungstests durchzuführen, um Systemschwächen regelmäßig zu untersuchen.

4. SEKTORSPEZIFISCHE ANFORDERUNGEN

Cybersicherheit im Gesundheitssektor

Die für die Gesundheitsbranche zuständige Zentralbehörde ist das Ministry of Health and Welfare (Ministerium für Gesundheit und Wohlfahrt). Gemäß der von diesem Ministerium am 24. April 2019 erlassenen Verwaltungsverordnung muss jeder vom Ministry of Health and Welfare beauftragte Anbieter kritischer Infrastrukturen vor jedem 31. Januar einen Cybersecurity Maintenance Plan vorlegen und vor jedem 31. Dezember über die Umsetzung des Plans Bericht erstatten. Das Ministerium wird den Anbieter kritischer Infrastrukturen gemäß dem CSMA auch einem Audit unterziehen.

Cybersicherheit im Finanzsektor

Finanzinstitutionen, Aussteller von elektronischen Wertkarten und Unternehmen, die elektronische Zahlungen erleichtern, müssen sich mit der Zentralbank und dem Joint Credit Information Center, JCIC, (Gemeinsamen Kreditinformationszentrum) abstimmen, um ihre Informationssicherheitsmaßnahmen zu standardisieren, und müssen zusätzlich bei der Central Deposit Insurance Corp (Einlagensicherung) und der Financial Supervisory Commission, FSC, (Finanzaufsichtskommission) Bericht erstatten oder sich registrieren lassen, wenn es zu regelmäßigen Audits oder Vorfällen von Verletzungen kommt.

Versicherungsanbieter, die ihre Geschäfte online abwickeln, müssen ISO 27001-zertifiziert sein und einen Mechanismus zur Bereinigung des Datenverkehrs gegen Distributed Denial of Service Attacks, DDoS, (verteilte Überlastattacken) einrichten, um Lizenzen zur Abwicklung von Geschäften zu erhalten.

Maßnahmen zur Cybersicherheit für Arbeitnehmer

Es gibt keine spezifischen Cybersicherheitsbestimmungen, die für das Verhältnis zwischen Arbeitgeber und Arbeitnehmer gelten. Der taiwanische Labor Standards Act schreibt vor, dass Arbeitgeber

verpflichtet sind, die Personalunterlagen für einen Zeitraum von fünf Jahren nach Beendigung des Arbeitsverhältnisses aufzubewahren. Arbeitgeber sind verpflichtet, die Vertraulichkeit dieser Unterlagen sicherzustellen, vorbehaltlich der allgemeinen Anforderungen des PDPA.

Cybersicherheit im Bildungssektor

Die zentrale Behörde, die für die Bildungsindustrie zuständig ist, ist das Ministry of Education (Bildungsministerium). Dieses erließ 2016 eine Verwaltungsvorschrift, die den Schutz der Cybersicherheit und persönlicher Daten regelt und die die Bezeichnung "Personal Data and Cyber Security Management Guidelines for Education" trägt. In dieser Verwaltungsvorschrift werden alle Schulen in die Klassen A (z.B. medizinische Universitäten), B (z.B. Universitäten) oder C (z.B. Grund- und weiterführende Schulen) eingeteilt, und sie richten ein "Personal Information Management System" oder "Information Security Management System" ein, um die Cybersicherheit und die persönlichen Daten zu verwalten und angemessene Ressourcen und Personal bereitzustellen, die das System regelmäßig warten und verbessern.

5. SANKTIONEN

Cyber Security Management Act

Artikel 20 des CSMA sieht Bußgelder in Höhe von 100.000 bis 1 Million TWD für Unternehmen vor, die es versäumen, innerhalb der von der jeweiligen Zentralbehörde, die für ihre Branche zuständig ist, gesetzten Frist korrigierende Maßnahmen vorzunehmen. Wenn ein Unternehmen es unterlassen hat, einen Vorfall im Bereich der Cybersicherheit zu melden, kann die zuständige Zentralbehörde gemäß Artikel 21 CSMA Bußgelder in Höhe von 300.000 bis 5 Millionen TWD verhängen und das Unternehmen auffordern, Verbesserungen vorzunehmen, die, wenn sie nicht rechtzeitig umgesetzt werden, zu weiteren Bußgeldern führen können.

6. ANDERE BEREICHE VON BEDEUTUNG

- z.B. Vertrauen, bemerkenswerte Vorfälle und Cyberattacken, Cybersicherheit von 5G-Netzwerken, Cybersicherheit von IoT/AI-basierten Systemen, Risikomanagement.

NCC gab 2019 5G-Lizenzen an Telekommunikationsbetreiber heraus und verlangt von ihnen derzeit, dass sie den Cybersecurity Maintenance Plan vorlegen und sich an die strengen Cybersicherheitsregeln in Bezug auf die Regulations for Administration of Mobile Broadband Businesses halten.

Während der COVID-19-Pandemie verbot die Zentralregierung allen Regierungsbehörden die Nutzung eines beliebten Videokonferenzdienstes aufgrund von Bedenken hinsichtlich der Cybersicherheit. Wegen der Neuartigkeit der allgemeinen Cybersicherheitsgesetzgebung in Taiwan war dies wahrscheinlich das erste Mal, dass ein solches pauschales Verbot erlassen wurde.

Autoren:

John EASTWOOD
john.eastwood@eiger.law

Wendy CHU
wendy.chu@eiger.law

Nathan SNYDER
nathan.snyder@eiger.law

Svea MATTHIESSEN
svea.matthiessen@eiger.law

Lloyd G. ROBERTS III
lloyd.roberts@eiger.law

DISCLAIMER

This article focuses on the requirements for private actors under the CSMA and related regulations, and the PDPA. It explicitly excludes cybersecurity regulations for military and intelligence agencies, and their contractors, insofar as these contractors have not also been designated as critical infrastructure providers by the competent authorities. Additionally, it also does not cover sector-specific regulations issued by the competent authorities for the relevant sectors