स्टैंडिंग कमिटी की रिपोर्ट का सारांश

साइबर सुरक्षा और साइबर अपराध की बढ़ती घटनाएं

- वित्त संबंधी स्टैंडिंग कमिटी (चेयर: श्री जयंत सिन्हा) ने 27 जुलाई, 2023 को 'साइबर सुरक्षा और साइबर/सफेदपोश अपराधों की बढ़ती घटनाएं' पर अपनी रिपोर्ट प्रस्तुत की। कमिटी के मुख्य निष्कर्षों और सुझावों में निम्नलिखित शामिल हैं:

- **सर्विस प्रोवाइडर्स का रेगुलेशन**: कमिटी ने कहा कि साइबर सुरक्षा मामलों में थर्ड पार्टी सर्विस प्रोवाइडर्स पर पर्याप्त नियंत्रण रखने में काफी चुनौतियां रही हैं। उसने सुझाव दिया कि इन सर्विस प्रोवाइडर्स, जिनमें बड़ी टेक और टेलीकॉम कंपनियां भी शामिल हैं, की निगरानी और नियंत्रण के लिए रेगुलेटरी शक्तियों को बढ़ाया जाए। कमिटी ने यह भी कहा कि बड़ी टेक कंपनियों को अपने सिस्टम को अधिक सुरक्षित बनाने के लिए भारतीय रिजर्व बैंक (आरबीआई) जैसे रेगुलेटर्स के इनपुट की अनदेखी नहीं करनी चाहिए।

- **क्रिटिकल पेमेंट सिस्टम्स**: क्रिटिकल पेमेंट सिस्टम्स में डाउनटाइम कस्टमर सर्विस को बाधित कर सकता है। हालांकि, वे इस समय रेगुलेटेड नहीं हैं। कमिटी ने सुझाव दिया कि इन पेमेंट सिस्टम्स को अपटाइम में सुधार करने और क्रिटिकल पेमेंट सिस्टम्स की समस्याओं को हल करने के लिए वित्तीय संस्थानों के साथ मिलकर काम करना चाहिए। मजबूत इंफ्रास्ट्रक्चर में निवेश, नियमित सुरक्षा आकलन और मामले के बाद प्रतिक्रिया तंत्र को स्थापित करके ऐसा किया जा सकता है।

- **रेगुलेटरी फ्रेमवर्क**: कमिटी ने कहा कि साइबर खतरों के खिलाफ महत्वपूर्ण वित्तीय इंफ्रास्ट्रक्चर को सुरक्षित करना महत्वपूर्ण है। उसने मजबूत नीतियों, नियमित जोखिम मूल्यांकन और घटना प्रतिक्रिया योजना को शामिल करते हुए एक व्यापक कानूनी फ्रेमवर्क की आवश्यकता पर जोर दिया। ऐसा रेगुलेटरी फ्रेमवर्क निम्नलिखित द्वारा स्थापित किया जा सकता है: (i) नए नियम लागू करना, (ii) साइबर सुरक्षा मामलों को संबोधित करने के लिए डिजिटल इंडिया कानूनी फ्रेमवर्क में संशोधन करना, या (iii) एक नया साइबर सुरक्षा कानून लाना।

- **साइबर प्रोटेक्शन अथॉरिटी**: कमिटी ने कहा कि साइबर सुरक्षा के वर्तमान रेगुलेटरी परिदृश्य में कई एजेंसियां और निकाय शामिल हैं। इसके लिए उच्च स्तरीय अंतर-मंत्रालयी समन्वय की जरूरत है। कोई भी केंद्रीय प्राधिकरण या एजेंसी पूरी तरह से साइबर सुरक्षा के लिए समर्पित नहीं है। कमिटी ने एक केंद्रीकृत साइबर प्रोटेक्शन अथॉरिटी (सीपीए) स्थापित करने का सुझाव दिया। अथॉरिटी राज्यों और निजी क्षेत्र की संस्थाओं के सहयोग से मजबूत साइबर सुरक्षा नीतियों, दिशानिर्देशों और सर्वोत्तम कार्य पद्धतियों को विकसित और कार्यान्वित करेगी।

- **छोटे वित्तीय संस्थानों के सामने चुनौतियां**: वाणिज्यिक बैंकों की तुलना में सहकारी बैंकों, गैर-बैंकिंग वित्तीय कंपनियों (एनबीएफसी) और अन्य छोटे प्रतिभागियों में साइबर सुरक्षा मामलों की संख्या अधिक है। सहकारी बैंकों और वाणिज्यिक बैंकों के बीच साइबर सुरक्षा ऑडिट के संबंध में भी काफी फर्क है। केवल 11% सहकारी बैंकों ने ऐसे ऑडिट किए हैं। एनबीएफसी, सहकारी बैंक, व्यापारी और विक्रेताओं के पास कर्मचारियों की सीमित संख्या है, और वे तकनीकी क्षमता के लिहाज से भी चुनौतियों का सामना करते हैं। कमिटी ने सुझाव दिया कि इन संस्थाओं को साइबर सुरक्षा इंफ्रास्ट्रक्चर, उन्नत जोखिम पहचान प्रणालियों और सुरक्षित डेटा स्टोरेज पद्धतियों में निवेश को प्राथमिकता देनी चाहिए। उन्हें कमजोरियों की पहचान करने के लिए नियमित ऑडिट और मूल्यांकन भी करना चाहिए।

- **डेटा शेयरिंग**: सर्च इंजनों और बड़ी टेक कंपनियों की मौजूदगी के साथ-साथ डिजिटल परिदृश्य के विस्तार ने साइबर अपराध के प्रति डिजिटल इकोसिस्टम की संवेदनशीलता को बढ़ा दिया है। इसके लिए सर्च इंजनों और ग्लोबल टेक कंपनियों की जिम्मेदारियों की स्पष्ट रूपरेखा तैयार करना जरूरी है। कमिटी ने सुझाव दिया कि एप्लिकेशन स्टोर्स के लिए उन सभी एप्लिकेशंस का विस्तृत मेटाडेटा और जानकारी साझा करना अनिवार्य किया जाना चाहिए जिन्हें वे अपने प्लेटफॉर्म पर होस्ट करते हैं। इस डेटा रेपोजिटरी से रेगुलेटर्स को यह शक्ति

तुषार चक्रवर्ती
tushar@prsindia.org

31 जुलाई, 2023

मिलेगी कि वे संभावित सुरक्षा संवेदनशीलता की पहचान करें और जरूरी उपाय करें। इसके अतिरिक्त टेक कंपनियों को निम्नलिखित करना चाहिए: (i) उन्हें अपने ऑपरेटिंग सिस्टम्स को नियमित अपडेट और पैच करना चाहिए, और (ii) अपने एप्लिकेशन स्टोर्स में मंजूरियों के लिए एक कठोर जांच प्रक्रिया लागू करनी चाहिए।

- **सेंट्रल नेगेटिव रजिस्ट्री**: कमिटी ने सेंट्रल नेगेटिव रजिस्ट्री बनाने का सुझाव दिया जिसे सीपीए मेनेटन करे। रजिस्ट्री में जालसाजों के एकाउंट्स की सूचना एकत्र होनी चाहिए। यह रजिस्ट्री बैंकों और एनबीएफसीज़ को उपलब्ध कराई जानी चाहिए जिससे वे सक्रिय रूप से धोखाधड़ी वाली गतिविधियों से जुड़े एकाउंट्स को खोलने से बचें।
- **जालसाजी पर हर्जाना**: वित्तीय क्षेत्र में साइबर अपराध पीड़ितों के लिए मौजूदा हर्जाने की व्यवस्था का दायरा और कवरेज सीमित है। हर्जाने के दावे दायर करने की प्रक्रिया जटिल है और यह पीड़ितों पर बर्डन ऑफ प्रूफ डालती है। कमिटी ने सुझाव दिया कि धोखाधड़ी के मामलों में ग्राहक को हर्जाना देना वित्तीय संस्थान की जिम्मेदारी होनी चाहिए।
- **सूचना प्रौद्योगिकी कानून**: कमिटी ने कहा कि सूचना प्रौद्योगिकी एक्ट, 2000 का पर्याप्त प्रवर्तन न होना, और ज्यादातर अपराधों की जमानती प्रकृति के कारण, धोखाधड़ी होती रहती है। कमिटी ने दंड के सख्त प्रावधानों और जमानत की कड़ी शर्तों को लागू करने तथा लोकल श्योरिटी के प्रावधानों पर विचार करने का सुझाव दिया।