भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 1743

जिसका उत्तर 27 जुलाई, 2022 को दिया जाना है ।

05 श्रावण, 1944 (शक)

साइबर हमले

1743. श्रीमती वांगा गीता विश्वनाथ :

डॉ. अरविन्द कुमार शर्मा :

श्री जी.एम. सिद्देश्वर :

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या विश्व में सबसे अधिक साइबर हमले भारत में, विशेष रूप से चीन द्वारा होते हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है और इस समस्या से निपटने के लिए क्या प्रयास किए जा रहे हैं;

(ख) क्या पिछले तीन वर्षों के दौरान सरकार द्वारा देश की साइबर सुरक्षा को मजबूत करने के लिए कोई सुरक्षा नीतियां शुरू की गई हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है और इसके तहत कितनी प्रगति हुई है और यदि नहीं, तो इसके क्या कारण हैं; और

(ग) क्या पिछले तीन वर्षों के दौरान सरकार द्वारा किसी व्यक्ति के डेटा की चोरी को रोकने के लिए कोई उपाय किए गए हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क): सरकार यह सुनिश्चित करने के लिए प्रतिबद्ध है कि भारत में इंटरनेट सभी उपयोगकर्ताओं के लिए खुला, सुरक्षित एवं विश्वसनीय और जवाबदेह हो । 80 करोड़ से अधिक भारतियों के इंटरनेट से जुड़े होने से, भारत दुनिया के सबसे बड़े जुड़े देशों में से एक है ।

गुमनामी के साथ सीमाहीन साइबर स्पेस के साथ, इंटरनेट के तेजी से विकास सहित , साइबर सुरक्षा की घटनाओं में वृद्धि एक वैश्विक घटना है। इसके अलावा, वर्ष 2022 में आईबीएम एक्स-फोर्स (एक खतरा आसूचना साझाकरण मंच) द्वारा प्रकाशित एक रिपोर्ट का हवाला देते हुए मीडिया लेख भी हैं, जिसमें कहा गया है कि भारत एशिया के ऐसे देशों में से एक था जिस पर सबसे अधिक साइबर हमले होते थे । साइबर सुरक्षा विक्रेताओं द्वारा ऐसी रिपोर्टों के निष्कर्ष आम तौर पर उनके उत्पादों द्वारा उत्पन्न डेटा पर आधारित होते हैं और ऐसे डेटा का विवरण उपलब्ध नहीं होता है और इसलिए सत्यापित नहीं किया जा सकता है।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) द्वारा दी गई रिपोर्ट और ट्रैक की गई जानकारी के अनुसार, वर्ष 2020, 2021 और 2022 (जून तक) के दौरान क्रमशः कुल 11,58, 208, 14,02,809 और 6,74,021 साइबर सुरक्षा घटनाएं देखी गई हैं।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट -इन) को उपलब्ध कराए गए लॉग के अनुसार, जिन कंप्यूटरों से हमले होते हैं, उनके इंटरनेट प्रोटोकॉल (आईपी) पते चीन सहित विभिन्न देशों के हैं ।

(ख): सरकार ने राष्ट्रीय साइबर सुरक्षा रणनीति (एनसीएसएस) का मसौदा तैयार किया है जो समग्र रूप से राष्ट्रीय साइबर स्पेस की सुरक्षा संबंधी समस्याओं का समाधान करता है। साइबर सुरक्षा रणनीति का दृष्टिकोण "भारत की समृद्धि के लिए एक सुरक्षित, सरंक्षित, भरोसेमंद, लचीला और जीवंत साइबर स्पेस सुनिश्चित करना" है।

गृह मंत्रालय (एमएचए) ने आईसीटी बुनियादी ढांचे में सूचना सुरक्षा उल्लंघनों/साइबर घुसपैठ को रोकने के लिए केंद्रीय मंत्रालयों/विभागों के साथ-साथ राज्य सरकारों/संघ राज्य क्षेत्रो को राष्ट्रीय सूचना सुरक्षा नीति और दिशानिर्देश (एनआईएसपीजी) जारी किए हैं।

राष्ट्रीय सूचना विज्ञान केंद्र नेटवर्क (निकनेट) के लिए साइबर सुरक्षा नीति लागू की गई है ।

(ग): सरकार ने साइबर सुरक्षा बढ़ाने और डेटा उल्लंघनों को कम करने के लिए निम्नलिखित प्रतिउपाय किए हैं:

(i) भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट -इन) डेटा उल्लंघनों की रोकथाम, डेटा लीक और डेटा उल्लंघनों के कारण पैदा हुए जोखिमों को कम करने और ऑनलाइन क्रेडेंशियल हासिल करने के लिए उपयोगकर्ताओं द्वारा अपनाई जाने वाली सर्वोत्तम प्रथाओं के संबंध में संगठनों को परामर्शी निदेश जारी करती है। सर्ट -इन ने डेटा सुरक्षा और धोखाधड़ी गतिविधियों को कम करने के लिए 70 परामर्श निदेश जारी किए हैं। इसके अलावा, सर्ट -इन नियमित आधार पर कंप्यूटर और नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्धताओ और प्रति-उपायों के बारे में अलर्ट और परामर्शी निदेश जारी करता है।

(ii) सर्ट -इन एक स्वचालित साइबर थ्रेट एक्सचेंज प्लेटफॉर्म संचालित करता है, जो उनके द्वारा सक्रिय खतरे को कम करने की कार्रवाई के लिए विभिन्न क्षेत्रों के संगठनों के साथ लगातार अलर्ट रूप से एकत्र करने, विश्लेषण करने और साझा करने के लिए है।

(iii) उपयोगकर्ताओं के लिए उनके डेस्कटॉप, मोबाइल/स्मार्ट फोन को सुरक्षित रखने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की गई हैं।

(iv) सरकार ने मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए एप्लिकेशन/बुनियादी ढांचे और अनुपालन हासिल करने के लिए उनकी प्रमुख भूमिकाओं और जिम्मेदारियों के संबंध में दिशानिर्देश जारी किए हैं।

(v) सभी सरकारी वेबसाइटों और एप्लिकेशन को उनकी होस्टिंग से पहले साइबर सुरक्षा के संबंध में लेखा परीक्षित किया जाता है। होस्टिंग के बाद भी वेबसाइटों और एप्लिकेशन का लेखा परीक्षण नियमित आधार पर किया जाता है।

(vi) सर्ट -इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखा परीक्षण करने के लिए 97 सुरक्षा लेखा परीक्षण संगठनों को पैनलबद्ध किया है।

(vii) सर्ट -इन ने केंद्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है।

(viii) साइबर सुरक्षा स्थिति और सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारियों का आकलन करने हेतु सक्षम बनाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित किए जाते हैं। सर्ट - इन द्वारा अब तक 67 ऐसे अभ्यास किए गए हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 886 संगठनों ने भाग लिया है ।

(ix) सर्ट -इन आईटी अवसंरचना को सुरक्षित रखने और साइबर हमलों को कम करने के संबंध में सरकार और महत्वपूर्ण क्षेत्र के संगठनों के नेटवर्क/सिस्टम प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2021 और 2022 (जून तक) के दौरान क्रमशः 5169 और 449 प्रतिभागियों को शामिल करते हुए 19 और 5 प्रशिक्षण कार्यक्रम आयोजित किए गए।

(x) सर्ट -इन साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र) संचालित करता है। केंद्र नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियों और सर्वोत्तम प्रथाओं के साथ-साथ दुर्भावनापूर्ण कार्यक्रमों का पता लगाने और उन्हें हटाने के लिए मुफ्त उपकरण प्रदान करता है।

(xi) सर्ट -इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक स्थितिजन्य जागरूकता उत्पन्न करने के लिए राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) की स्थापना की है। एनसीसीसी का चरण-I प्रचालनरत है ।

(xii) सर्ट - इन अंतरराष्ट्रीय सर्ट, विदेशी संगठनों और सेवा प्रदाताओं के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ सहयोग करता है, काम करता है और घटना प्रतिक्रिया उपायों का समन्वय करता है।

(xiii) सर्ट -इन अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से नियमित रूप से सूचना का प्रसार करता है और साइबर सुरक्षा और सरंक्षा पर सुरक्षा युक्तियों को साझा करता है। सर्ट -इन ने अक्टूबर 2021 में साइबर सुरक्षा जागरूकता माह और 8 फरवरी 2022 को सुरक्षित इंटरनेट दिवस के दौरान सोशल मीडिया प्लेटफॉर्म और वेबसाइटों पर पोस्टर और वीडियो का उपयोग करके सुरक्षा युक्तियों को पोस्ट करके नागरिकों के लिए विभिन्न कार्यक्रमों और गतिविधियों का आयोजन किया। सर्ट ने सीडैक के सहयोग से माईगव प्लेटफॉर्म पर वीडियो और क्विज़ के माध्यम से सामान्य ऑनलाइन सुरक्षा, सोशल मीडिया जोखिम और सुरक्षा, मोबाइल से संबंधित धोखाधड़ी और सुरक्षा, सुरक्षित डिजिटल भुगतान प्रथाओं आदि जैसे विषयों को शामिल करने वाले नागरिकों के लिए ऑनलाइन जागरूकता अभियान चलाया है।

(xiv) सर्ट -इन, भारतीय रिजर्व बैंक (आरबीआई) और डिजिटल इंडिया संयुक्त रूप से डिजिटल इंडिया प्लेटफॉर्म के माध्यम से 'वित्तीय धोखाधड़ी से सावधान रहें और जागरूक रहें' पर एक साइबर सुरक्षा जागरूकता अभियान चलाते हैं।

(xv) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में बच्चों, माता-पिता और सामान्य उपयोगकर्ताओं के लिए विशिष्ट पुस्तकें, वीडियो और ऑनलाइन सामग्री विकसित की जाती हैं, जिन्हें "www.infosecawareness.in" और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित किया जाता है।

(xvi) राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) संवेदनशील सूचनाओं की सुरक्षा के लिए नेटवर्क और एप्लिकेशन दोनों स्तरों पर लागू की जाने वाली तकनीकों संबंधी प्रथाओ, प्रक्रियाओं के रूप में स्तरित सुरक्षा दृष्टिकोण अपनाता है। इसे आवधिक अनुपालन, लेखा परीक्षा और सुभेद्यता मूल्यांकन के माध्यम से और सुदृढ़ किया जाता है।

****