भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या3822

जिसका उत्तर 18दिसम्बर, 2024 को दिया जाना है।

27अग्रहायण,1946 (शक)

साइबर की रोकथाम

3822.श्री तनुज पुनिया:

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

(क) क्या सरकार ने हाल ही में साइबर हमलों को रोकने के लिए कुछ उपाय किए हैं जिनमें विभिन्न एजेंसियों के साथ समन्यवय स्थापित करने के लिए अंतर-विभागीय पैनल का गठन शामिल है और यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ख) विगत तीन वर्षों के प्रत्येक वर्ष के दौरान साइबर सुरक्षा संबंधी कितनी घटनाओं की सूचना मिली है;

(ग) क्या उक्त मामलों का पता भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल द्वारा लगाया गया था;

(घ) यदि हां, तो तत्संबंधी ब्यौरा क्या है और इस संबंध में क्या आवश्याक कार्रवाई की गई है और;

(ङ) क्या विभिन्न क्षेत्रों के संगठनों के साथ चेतावनियां साझा करने के लिए कोई सक्रिय उपाय किए गए है और यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क):सरकार यह सुनिश्चित करने के लिए प्रतिबद्ध है कि भारत में इंटरनेट की सुविधा इसके उपयोगकर्ताओं के लिए खुला, सुरक्षित, विश्वसनीय तथा जवाबदेह हो। सरकार विभिन्न साइबर सुरक्षा खतरों और चुनौतियों से पूरी तरह अवगत है और उसने साइबर हमलों को रोकने के लिए निम्नलिखित उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं:

i. विभिन्न एजेंसियों के बीच समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) के अंतर्गत राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी) की व्यवस्था की गई है।

ii. सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के अंतर्गत, सरकार ने देश में महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है।

iii. सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70बी के प्रावधानों के अंतर्गत, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को साइबर सुरक्षा घटनाओं से निपटने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

iv. गृह मंत्रालय (एमएचए) ने समन्वित और प्रभावी तरीके से साइबर अपराधों से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) की स्थापना की है।

v. सर्ट-इन ने सुरक्षित एंव विश्वसनीय इंटरनेट सुविधा सुनिश्चित करने के लिए सूचना सुरक्षा पद्धतियों, प्रक्रियाओं के बारे में तथा साइबर घटनाओं के निवारण और ऐसी घटनाओं क संबंध में दी जा रही अथवा ध्यान में लाई जा रही सूचनाओं के बारे में 6 घंटों के भीतर सर्ट-इन को अवगत कराने हेतु सर्ट-इन द्वारा सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70बी की उप-धारा(6) के अंतर्गत अप्रैल, 2022 में साइबर सुरक्षा निर्देश जारी किये गये थे।

vi. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष

आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा ऑडिटिंग जैसे डोमेन शामिल हैं।

vii. सर्ट-इनने नवंबर 2023 में विभिन्न मंत्रालयों को एक एडवाइजरी जारी की थी, जिनमें संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना को प्रोसेस करने वाली सभी संस्थाओं द्वारा साइबर सुरक्षा को मजबूत करने के लिए किए जाने वाले उपायों की रूपरेखा का उल्लेख किया गया है।

viii. सर्ट-इनसूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम करने के बारे में सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के नेटवर्क और सिस्टम प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित किये जाते हैं।2024 (अक्टूबर तक) में 20 प्रशिक्षण कार्यक्रमों में कुल 9,807 अधिकारियों को प्रशिक्षित किया गया है।

ix. सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपायों के संबंध में निरंतर अलर्ट और एडवाइजरीज जारी करता है।

x. सरकारी और महत्वपूर्ण क्षेत्रों से संबंधित संगठनों की साइबर सुरक्षा की स्थिति और तैयारियों का आकलन करने के लिए साइबर सुरक्षा मॉक ड्रिल आयोजित की जा रही हैं। सर्ट-इन द्वारा अब तक 104 ऐसी मोकड्रिल्स आयोजित की गयी हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 1420 संगठनों द्वारा भाग लिया जा चुका है।

xi. सर्ट-इन द्वारा विभिन्न मंत्रालयों को एक एडवाइजरी जारी करके संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना कोप्रोसेस करने वाली सभी संस्थाओं की ओर से साइबर सुरक्षा को मजबूत करने के लिए उठाए जाने वाले उपायों की रूपरेखा बताई गई है।

(ख) से (ङ): सर्ट-इन को सूचित की गई और उसके द्वरा ट्रैक की गई जानकारी के अनुसार, पिछले तीन वर्षों में साइबर सुरक्षा से संबंधित हुई घटनाओं की कुल संख्या नीचे दी गई है:

वर्ष	साइबर सुरक्षा घटनाओं की संख्या
2021	14,02,809
2022	13,91,457
2023	15,92,917

विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट साझा करने के लिए निम्नलिखित उपाय किए गए हैं:

i. सर्ट-इन द्वारा सक्रियता पूर्वक अनुरूपी अलर्ट्स प्राप्त करने, उनका विश्लेषण करने तथा संबंधित क्षेत्रों के साथ इन अलर्ट्स को साझा करने के लिए एक स्वचालित साइबर जोखिम खुफिया आदान-प्रदान प्लेटफार्म का संचालन किया जाता है, ताकि इन संगठनों द्वारा जोखिम कम करने की तीव्रतापूर्ण कार्रवाई की जा सके।

ii. सर्ट-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य किया जाता है। एनसीसीसी साइबर सुरक्षा खतरों को कम करने के लिए कार्रवाई करने के लिए साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

iii. साइबर स्वच्छता केंद्र (सीएसके) सर्ट-इनद्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है, जो स्वच्छ भारत संबंधि विचार को साइबर स्पेस तक विस्तारित करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मौलवेयर विश्लेषण केंद्र है जो दुर्भावनापूर्ण तैयार किये गए कार्यक्रमों का का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है, तथा नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम प्रविधियाँ भी उपब्लध कराता है।

iv. राष्ट्रीय सूचना विज्ञान केन्द्र (एनआईसी) ने सरकारी नेटवर्क से जुड़े सुरक्षा मुद्दों की पहचान करने के लिए थ्रेट इंटेलिजेंस प्लेटफॉर्म सहित उन्नत सुरक्षा उपकरण तैनात किए हैं।

v. एनसीआईआईपीसी साइबर हमलों और साइबर आतंकवाद से बचाव के उपाय करने के लिए महत्वपूर्ण सूचना अवसंरचना (सीआईआईएस)/संरक्षित प्रणालियों (पीएस) वाले संगठनों को खतरे की खुफिया जानकारी, स्थितिजन्य जागरूकता, अलर्टस और एडवाइजरीज के साथ-साथ सुभेद्यताओं के बारे में भी जानकारी प्रदान करता है।

vi. सर्ट-इन नवीनतम साइबर खतरों, सर्वोत्तम कार्य प्रणालियों पर सूचना का आदान-प्रदान करने तथा संयुक्त क्षमता निर्माण कार्यक्रम आयोजित करने के लिए उद्योग जगत के साथ सहयोग करता है।

vii. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय द्वारा सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित किये जाते हैं। साइबर स्वच्छता और डीपफेक सहित साइबर सुरक्षा के विभिन्न पहलुओं पर हैंडबुक, लघु वीडियो, पोस्टर, ब्रोशर, बच्चों के लिए कार्टून कहानियां, सलाह आदि के रूप में जागरूकता सामग्री www.staysafeonline.in, www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती है।

*****