भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 762

जिसका उत्तर 7 फरवरी, 2024 को दिया जाना है।

18 माघ, 1945 (शक)

साइबर हमलों से बचाव

762. श्री मनोज तिवारी:

डॉ. निशिकांत दुबे:

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 विभिन्न एजेंसियों के साथ समन्वय करने के लिए अंतर-विभागीय पैनल के सृजन सहित कुछ उपाय किए हैं;

(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ग) विगत तीन वर्षों के दौरान वर्ष-वार साइबर सुरक्षा संबंधी कितनी घटनाओं की सूचना मिली है;

(घ) क्या उक्त मामलों का भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) द्वारा पता लगाया गया था और आवश्यक कार्रवाई की गई थी और यदि हां, तो तत्संबंधी ब्यौरा क्या है; और

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

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) और (ख): सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित और विश्वसनीय और उत्तरदायी इंटरनेट सुनिश्चित करना है। सरकार विभिन्न साइबर सुरक्षा खतरों और चुनौतियों से पूरी तरह परिचित और जागरूक है और उसने साइबर सुरक्षा स्थिति को बढ़ाने और साइबर हमलों को रोकने के लिए निम्नलिखित उपाय किए हैं:

(i) इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (सीआईआरटी-इन) ने अप्रैल 2022 में धारा 70ख के अंतर्गत ऐसी घटनाओं के नोटिस होने या नोटिस में लाए जाने के छह घंटे के भीतर सीआईआरटी-इन को साइबर घटनाओं की अनिवार्य रिपोर्टिंग के लिए निर्देश जारी किए।

(ii) सीआईआरटी-इन ने दिसंबर 2022 में स्वास्थ्य क्षेत्र की संस्थाओं के लचीलेपन को बढ़ाने के लिये सर्वोत्तम प्रथाओं पर एक विशेष सलाह जारी की और स्वास्थ्य और परिवार कल्याण मंत्रालय (एमओएचएफडब्ल्यू) से देश की सभी अधिकृत चिकित्सा देखभाल संस्थाओं और सेवा प्रदाताओं को इसका प्रसार करने का अनुरोध किया है।

(iii) सीईआरटी-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए

हैं, 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।

(iv) साइबर सुरक्षा नीतियों के समन्वय, देखरेख और अनुपालन के लिए राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी) का कार्यालय स्थापित किया गया है। एनसीएससी के कार्यों में, अन्य विषयों के साथ-साथ, उत्तरदायित्व वाले क्षेत्रों में नोडल एजेंसियों द्वारा साइबर सुरक्षा के लिए कार्य योजनाओं को सलाह देना और कार्यान्वयन सुनिश्चित करना शामिल है।

(v) साइबर सुरक्षा जोखिमों को कम करने के लिए , दूरसंचार क्षेत्र पर राष्ट्रीय सुरक्षा निर्देश 15 जून 2021 से अनिवार्य कर दिया गया है।

(vi) सीईआरटी-इन विभिन्न क्षेत्रों के संगठनों के साथ सक्रिय खतरे को कम करने की कार्रवाइयों के लिए सक्रिय रूप से एकत्रित करने, विश्लेषण करने और साझा करने के लिए एक स्वचालित साइबर खतरा विनिमय मंच संचालित करता है।

(vii) सीईआरटी-इन निरंतर आधार पर कंप्यूटर और नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों/अतिसंवेदनशीलता और जवाबी उपायों के संबंध में अलर्ट और सलाह जारी करता है।

(viii) सीईआरटी-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में स्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केंद्र की स्थापना की है।

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

(x) सीईआरटी-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का सहयोग और ऑडिट करने के लिए 177 सुरक्षा ऑडिटिंग संगठनों को सूचीबद्ध किया है।

(xi) सरकार और महत्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा स्थिति और तैयारियों का आकलन करने में सक्षम बनाने के लिए साइबर सुरक्षा मॉक ड्रिल आयोजित की जाती है। सीईआरटी-इन द्वारा अब तक 87 ऐसे अभ्यास आयोजित किए जा चुके हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 1173 संगठनों ने भाग लिया।

(xii) दुर्भावनापूर्ण कार्यक्रमों का पता लगाने और उन्हें हटाने के लिए मुफ्त टूल और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास प्रदान करने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र)का संचालन सर्ट-इन द्वारा किया जाता है।

(xiii) उपयोगकर्ताओं के लिए उनके डेस्कटॉप और मोबाइल फोन को सुरक्षित करने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की गई हैं।

(ग): सीईआरटी-इन द्वारा रिपोर्ट की गई और ट्रैक की गई जानकारी के अनुसार, वर्ष 2021, 2022 और 2023 के दौरान क्रमशः कुल 14,02,809 13,91,457 और 15,92,917 साइबर सुरक्षा घटनाएं देखी गईं।

(घ): सीईआरटी-इन विभिन्न क्षेत्रों में संस्थाओं के नेटवर्क में मैलवेयर संक्रमण और अतिसंवेदनशीलताओं के बारे में अपने स्थितिजन्य जागरूकता प्रणालियों और थ्रेट इंटेलिजेंस स्रोतों से इनपुट प्राप्त करता है और उपचारात्मक उपायों के लिए संबंधित संगठनों और क्षेत्रीय कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीमों (सीएसआईआरटी) को अलर्ट जारी करता है। सीईआरटी-इन प्रभावित संगठनों, सेवा प्रदाताओं के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का सहयोग, कार्य और समन्वय करता है।

(ङ): सरकार ने विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट साझा करने के लिए निम्नलिखित सक्रिय उपाय किए हैं:

(i) सीईआरटी-इन विभिन्न क्षेत्रों के संगठनों के साथ सक्रिय खतरे को कम करने की कार्रवाइयों के लिए सक्रिय रूप से एकत्रित करने, विश्लेषण करने और साझा करने के लिए एक स्वचालित साइबर-खतरा विनिमय मंच संचालित करता है।

(ii) सीईआरटी-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक स्थितिजन्य जागरूकता पैदा करने और व्यक्तिगत संस्थाओं द्वारा सक्रिय, निवारक और सुरक्षात्मक कार्यों के लिए समय पर जानकारी साझा करने में सक्षम बनाने के लिए राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) की स्थापना की है।

(iii) दुर्भावनापूर्ण प्रोग्रामों का पता लगाने और उन्हें हटाने के लिए मुफ्त टूल और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास प्रदान करने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र) संचालित करता है।

(iv) नेशनल क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (एनसीआईआईपीसी) का विश्लेषणात्मक केंद्र वास्तविक समय में खतरे की खुफिया जानकारी और स्थितिजन्य जागरूकता प्रदान करता है, जिसके आधार पर क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर/संरक्षित सिस्टम इकाइयों को नियमित अलर्ट और अनुरूप सलाह भेजी जाती है।

****