भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 3122

जिसका उत्तर 19 मार्च, 2025 को दिया जाना है

28 फाल्गुन, 1946 (शक)

बग 'फ्री वायरस'

3122. श्री ईश्वरस्वामी के.:

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

(क) क्या यह सच है कि एक परिष्कृत बग 'फ्री वायरस' ने देश में कुछ अति संवेदनशील प्रतिष्ठानों को संक्रमित कर दिया है;

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

(ग) सरकार द्वारा 'फ्री वायरस' की समस्या से निपटने और देश में संवेदनशील प्रतिष्ठानों की सुरक्षा के लिए क्या कदम उठाए गए हैं ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) और (ख): सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70 बी के अनुसार, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) साइबर सुरक्षा घटना प्रतिक्रिया गतिविधियों के समन्वय के लिए राष्ट्रीय एजेंसी है। सर्ट-इन अपनी स्थितिजन्य जागरूकता प्रणालियों और जोखिमों से संबंधित खुफिया स्रोतों से विभिन्न क्षेत्रों की संस्थाओं के नेटवर्क में मैलवेयर संक्रमण और कमजोरियों के बारे में इनपुट प्राप्त करता है और उपचारात्मक उपायों के लिए संबंधित संगठनों और क्षेत्रीय कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल (सीएसआईआरटी) को अलर्ट जारी करता है। सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70ए के अनुसार, सरकार ने देश में महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना बुनियादी ढांचा संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है। एनसीआईआईपीसी के अनुसार अधिसूचित की गई महत्वपूर्ण सूचना अवसंरचनाओं के संबंध में ऐसी कोई घटना की जानकारी नहीं मिली है।

(ग): सरकार ने साइबर सुरक्षा स्थिति को बढ़ाने और मैलवेयर हमलों सहित साइबर हमलों को रोकने के लिए निम्नलिखित उपाय किए हैं:

(i) साइबर स्वच्छता केंद्र (सीएसके) सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है जो स्वच्छ भारत के विजन को साइबर स्पेस तक विस्तारित करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है जो दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है। यह नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम कार्यपद्धतियां भी प्रदान करता है।

(ii) सर्ट-इन कंप्यूटरों और नेटवर्कों की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों तथा प्रतिउपायों के संबंध में निरंतर अलर्ट और परामर्श जारी करता है।

(iii) सर्ट-इन एक स्वचालित साइबर खतरा विनिमय प्लेटफॉर्म संचालित करता है, जो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है, ताकि वे खतरा न्यूनीकरण के लिए सक्रिय रूप से कार्रवाई कर सकें।

(iv) 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 करता 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।

(v) सर्ट-इन ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70बी की उपधारा (6) के तहत सुरक्षित एवं विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा पद्धतियों, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग से संबंधित साइबर सुरक्षा निर्देश जारी किए।

(vi) सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा पद्धतियों पर दिशानिर्देश जारी किए हैं, जिनमें 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-इन ने सितंबर 2023 में सुरक्षित एप्लिकेशन डिज़ाइन, विकास और कार्यान्वयन और संचालन के लिए दिशानिर्देश जारी किए हैं। सर्ट-इन ने अक्टूबर 2024 में संस्थाओं, विशेष रूप से सार्वजनिक क्षेत्र, सरकार, आवश्यक सेवाओं, सॉफ़्टवेयर निर्यात और सॉफ़्टवेयर सेवा उद्योग में शामिल संगठनों के लिए सॉफ़्टवेयर बिल ऑफ़ मैटेरियल्स (एसबीओएम) दिशानिर्देश भी जारी किए हैं। एसबीओएम संगठनों को यह जानने में मदद करता है कि उनके सॉफ़्टवेयर या परिसंपत्तियों में कौन से घटक हैं, जिससे कमज़ोरियों की पहचान करना और उन्हें ठीक करना आसान हो जाता है।

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

(ix) सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 200 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

(x) सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा स्थिति और तैयारियों का आकलन करने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जा रही हैं। सर्ट-इन द्वारा अब तक 109 ऐसे ड्रिल्स आयोजित किए गए हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 1438 संगठनों ने भाग लिया।

(xi) सर्ट-इन सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम करने के बारे में नेटवर्क और सिस्टम प्रशासकों और सरकारी और महत्वपूर्ण क्षेत्र संगठनों के मुख्य सूचना सुरक्षा कार्मिकों के लिए नियमित

प्रशिक्षण कार्यक्रम आयोजित करता है। 2024 में 23 प्रशिक्षण कार्यक्रमों में कुल 12,014 अधिकारियों को प्रशिक्षित किया गया है।

******