भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2340

जिसका उत्तर 15 मार्च, 2023 को दिया जाना है।

24 फाल्गुन, 1944 (शक)

साइबर हमलों से बचाव

2340. श्री मितेष पटेल (बकाभाई) :

श्रीमती शारदा अनिल पटेल :

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

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

(ख) पिछले तीन वर्षों के दौरान रिपोर्ट की गई साइबर सुरक्षा घटनाओं की वर्ष-वार संख्या कितनी है;

(ग) क्या उक्त मामलों को भारतीय कंम्प्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-इन) द्वारा ट्रैक किया गया था और आवश्यक कार्रवाई की गई थी और यदि हां, तो तत्संबधी ब्यौरा क्या है; और

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

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क): सरकार साइबर सुरक्षा के बढ़ते खतरों और हमलों के बारे में पूरी तरह से जागरूक और परिचित है, और डिजिटल नागरिकों के लिए समग्र रूप से सुरक्षित और विश्वसनीय सुनिश्चित करने के लिए साइबर हमलों की रिपोर्टिंग को रोकने और त्वरित करने के लिए निम्नलिखित उपाय किए हैं:

(i) सर्ट-इन ने अप्रैल 2022 में धारा 70 ख के तहत साइबर घटनाओं की अनिवार्य रिपोर्टिंग के लिए ऐसी घटनाओं के नोटिस में आने या नोटिस में लाए जाने के छह घंटे के भीतर सर्ट-इन को निर्देश जारी किए।

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

(iii) केंद्र सरकार के मंत्रालयों और विभागों के लिए काम करने वाले आउटसोर्स, संविदात्मक और अस्थायी कर्मचारियों सहित सभी सरकारी कर्मचारियों के पालन के लिए सितंबर 2022 में साइबर सुरक्षा श्रेष्ठ पद्धतियां जारी की गई हैं।

(iv) गृह मंत्रालय ने रैंसमवेयर खतरों से प्रभावी ढंग से निपटने के लिए रणनीति तैयार करने और हितधारकों द्वारा सक्रिय और उत्तरदायी प्रणाली स्थापित करने के लिए कई हितधारकों को शामिल करते हुए राष्ट्रीय काउंटर रैंसमवेयर टास्कफोर्स बनाया है। टास्कफोर्स में सहयोग और कूटनीति, घटना प्रतिक्रिया, सुरक्षा क्लस्टर, जागरूकता और क्षमता निर्माण पर कार्य समूह शामिल हैं।

(v) सर्ट -इन अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से साइबर सुरक्षा और संरक्षा पर सूचना का प्रसार करता है और सुरक्षा युक्तियों को साझा करता है। सर्ट -इन ने सोशल मीडिया प्लेटफॉर्म और वेबसाइटों पर सुरक्षा टिप्स और वीडियो पोस्ट करके 8.2.2022 को सुरक्षित इंटरनेट दिवस और अक्टूबर 2022 में साइबर सुरक्षा जागरूकता माह के दौरान नागरिकों के लिए विभिन्न कार्यक्रमों और गतिविधियों का आयोजन किया है।

(vi) सर्ट -इन ने सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग (सी-डैक) के सहयोग से नागरिकों के लिए एक ऑनलाइन जागरूकता अभियान चलाया है, जिसमें सामान्य ऑनलाइन सुरक्षा, सोशल मीडिया जोखिम और सुरक्षा, मोबाइल से संबंधित धोखाधड़ी और माय गव प्लेटफॉर्म पर वीडियो और क्विज़ के माध्यम से सुरक्षा, सुरक्षित डिजिटल भुगतान प्रथाओं आदिजैसे विषयों को शामिल किया गया है।

(vii) सर्ट-इन, निरंतर आधार पर, कंप्यूटर और नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपायों के बारे में अलर्ट और सलाह जारी करता है। उपयोगकर्ताओं को अपने डेस्कटॉप और मोबाइल फोन को सुरक्षित रखने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की जाती हैं।

(viii) सर्ट-इन नेटवर्क और सिस्टम प्रशासकों और सरकारी और महत्वपूर्ण क्षेत्र के संगठनों के सीआईएसओ के लिए नियमित रूप से सूचना प्रौद्योगिकी के बुनियादी ढांचे को सुरक्षित करने और साइबर हमलों को कम करने के लिए प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2021 और 2022 के दौरान कुल 42 प्रशिक्षण कार्यक्रम आयोजित किए गए, जिनमें 11,486 प्रतिभागियों को शामिल किया गया।

(ix) सरकार और महत्वपूर्ण क्षेत्रों में साइबर सुरक्षा मुद्रा और संगठनों की तैयारी के आकलन को सक्षम करने के लिए साइबर सुरक्षा मॉक ड्रिल आयोजित की जा रही है। सर्ट-इन द्वारा अब तक 74 ऐसे अभ्यास किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के 990 संगठनों ने भाग लिया।

(ख) और **(ग)**: सर्ट-इन को दी गई और ट्रैक की गई सूचना के अनुसार, वर्ष 2020, 2021 और 2022 के दौरान क्रमशः कुल 11,58,208, 14,02,809 और 13,91,457 साइबर सुरक्षा घटनाएं देखी गईं। सर्ट-इन अपने स्थितिजन्य जागरूकता प्रणालियों से इनपुट प्राप्त करता है और विभिन्न क्षेत्रों में संस्थाओं के नेटवर्क में मैलवेयर संक्रमण और सुभेद्यता के बारे में खतरे की खुफिया जानकारी प्राप्त करता है और उपचारात्मक उपायों के लिए संबंधित संगठनों और क्षेत्रीय कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीमों (सीएसआईआरटी) को अलर्ट जारी करता है।

(घ): सभी क्षेत्रों के संगठनों के साथ अलर्ट साझा करने के लिए निम्नलिखित उपाय किए गए हैं:

(i) सर्ट-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में स्थितिजन्य जागरूकता उत्पन्न करने के लिए राष्ट्रीय साइबर समन्वय केंद्र की स्थापना की है। यह सक्रिय रूप से एकत्र करने,

विश्लेषण करने और उनके द्वारा सक्रिय खतरे शमन कार्यों के लिए क्षेत्रों में संगठनों के साथ अनुरूप अलर्ट साझा करने के लिए एक स्वचालित साइबर-खतरा विनिमय मंच संचालित करता है।

(ii) सर्ट-इन दुर्भावनापूर्ण प्रोग्रामों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) का संचालन करता है और इसे हटाने के लिए मुफ्त उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा टिप्स और श्रेष्ठ पद्धति प्रदान करता है।

****