भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या 2504

जिसका उत्तर 16 मार्च, 2018 को दिया जाना है।

25 फाल्गुन, 1939 (शक)

साइबर सुरक्षा के जोखिमों में वृद्धि

2504. श्रीमती जया बच्चन :

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

(क) क्या इंटरनेट से उत्पन्न साइबर सुरक्षा के जोखिमों में निरंतर वृद्धि हो रही है;

(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है और इस संबंध में प्राप्त हुई सरकारी/निजी रिपोर्टों तथा इस संबंध में सरकार की प्रतिक्रिया का क्या ब्यौरा है;

(ग) क्या यह सच है कि भारत में अधिकाधिक संगठनों का मानना है कि 'क्लाउड' पर भंडारित उनका सारा डेटा सुरक्षित नहीं है;

(घ) यदि हां, तो तत्संबंधी ब्यौरा क्या है; और

(ड.) सरकार द्वारा सारे डेटा की सुरक्षा सुनिश्चित करने के लिए सुरक्षा रणनीति तथा प्रणालियों में बदलाव तथा उन्नयन करके साइबर धोखाधड़ी को कम करने के लिए आगामी पीढ़ी की सुरक्षा को अंगीकार करने के लिए किए जा रहे सुधारात्मक उपायों का ब्यौरा क्या है ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री के.जे. एल्फोंस)

(क) और **(ख)** : सूचना प्रौद्योगिकी और संबंधित सेवाओं के प्रसार के साथ ही विश्व के अन्य देशों की तरह देश में साइबर सुरक्षा घटनाओं के साथ साइबर सुरक्षा खतरों में भी वृद्धि हुई है। भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को रिपोर्ट की गई और उसके द्वारा ट्रैक की गई सूचना के अनुसार वर्ष 2014, 2015, 2016 और 2017 के दौरान क्रमश: कुल 44679, 49455, 50362 और 53081 साइबर सुरक्षा संबंधी घटनाएं रिपोर्ट की गई। साइबर सुरक्षा संबंधी घटनाओं में फिशिंग, स्कैनिंग/जांच पड़ताल, वेबसाइट इंटरूजन और विरुपण, वायरस/विद्वेषपूर्ण कोड, सेवा की मनाही इत्यादि शामिल हैं। पिछले कुछ समय के दौरान घटनाओं की प्रकृति और तरीके और अधिक संवेदनशील और जटिल हो गए हैं। सूचना प्रौद्योगिकी की गतिशील प्रकृति के अनुरूप साइबर हमलों का पता लगाने और उनकी रोकथाम करने के लिए सतत प्रयास किए जाने अपेक्षित हैं।

(ग) और **(घ)** : ऐसी कोई अध्ययन रिपोर्ट इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के संज्ञान में नहीं लाई गई है।

(ड.) : सरकार ने साइबर सुरक्षा के मुद्दे का समाधान करने के लिए बहुत सारे विधिक, तकनीकी और प्रशासनिक नीतिगत उपाय किए हैं। इसमें आईटी अधिनियम, 2000 के अंतर्गत (i) राष्ट्रीय साइबर सुरक्षा नीति (ii) साइबर सुरक्षा बढ़ाने हेतु फ्रेमवर्क (iii) सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 का अधिनियमन (iv) भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) की स्थापना और (v) राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) शामिल हैं :

i. सरकार ने देश में महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70क के प्रावधानों के अनुसार राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है। एनसीआईआईपीसी सुरक्षा के लिए खतरे संबंधी आसूचना, दिशानिर्देश, उत्कृष्ट प्रणालियों और फ्रेमवर्कों को साझा करते हुए सभी प्रकार के हमलों और आक्रमणों के प्रति सुभेद्यताओं को कम करने के लिए महत्वपूर्ण सूचना अवसंरचना क्षेत्र के संगठनों को परामर्श नियमित रूप से देता आ रहा है और उन्हें नीतियों और सुरक्षा रणनीतियों से संबंधित मार्गदर्शन दे रहा है। इसके अलावा, सीआईआई संगठनों में साइबर स्वच्छता को बेहतर बनाने के लिए प्रशिक्षण और जागरूकता कार्यक्रम भी नियमित रूप से संचालित किए जा रहे हैं।

ii. सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों तथा महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए सरकार ने साइबर हमलों से निपटने के लिए साइबर आपदा प्रबंधन योजना तैयार की है।

iii. सरकार ने अनुप्रयोगों अवसंरचना की सुरक्षा के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए सामान्य दिशानिर्देश और अनुपालन के लिए उनकी प्रमुख भूमिकाओं तथा जिम्मेदारियों से संबंधित निर्देश जारी किए हैं।

iv. भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट -इन) ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन की सहायता और लेखापरीक्षा के लिए 67 साइबर सुरक्षा लेखापरीक्षा संगठनों को पैनलबद्ध किया है।

v. सरकारी और महत्वपूर्ण क्षेत्रों के संगठनों की साइबर सुरक्षा की स्थिति और तैयारी का मूल्यांकन करने में उन्हें सक्षम बनाने के लिए नियमित रूप से साइबर सुरक्षा मॉक ड्रिल संचालित की जा रही हैं। अब तक भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) द्वारा इस प्रकार की 15 मॉकड्रिल संचालित की गई हैं जिनमें वित्त क्षेत्र सहित रक्षा, ऊर्जा, दूरसंचार, परिवहन, विद्युत, अंतरिक्ष आईटी/आईटीईएस इत्यादि क्षेत्रों जैसे विभिन्न क्षेत्रों के 148 संगठनों ने भाग लिया। इसके साथ ही भारतीय रिजर्व बैंक और बैंकिंग प्रौद्योगिकी विकास और अनुसंधान संस्थान के समन्वय में 3 ड्रिलों का संचालन किया गया है।

vi. सर्ट-इन सरकार और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सुरक्षा अधिकारी (सीआईएसओ) और नेटवर्क/प्रणाली प्रशासकों के लिए आईटी अवसंरचना को सुरक्षित करने और साइबर हमलों के उन्मूलन के लिए नियमित रूप से साइबर सुरक्षा प्रशिक्षण कार्यक्रम आयोजित कर रहा है। वर्ष 2017 के दौरान ऐसे 22 प्रशिक्षण कार्यक्रमों का आयोजन किया गया जिसमें 610 भागीदारों ने हिस्सा लिया।

vii. सरकार ने विद्यमान और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक परिस्थितिजन्य जागरूकता पैदा करने और अलग-अलग इकाइयों द्वारा सक्रिय, निवारक और सुरक्षात्मक कार्रवाई करने के लिए समय पर सूचना साझा करने के लिए राष्ट्रीय साइबर समन्वय केन्द्र (एनसीसीसी) की स्थापना शुरू की है। एनसीसीसी के चरण-I को प्रचालनरत किया गया है।

viii. सरकार ने साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एण्ड मालवेयर एनालिसिस सेंटर) स्थापित किया है। यह केंद्र बैंकों के साथ-साथ सामान्य प्रयोक्ताओं को मैलीशियस प्रोग्रामों का पता लगाने और उन्हें हटाने के लिए नि:शुल्क टूल उपलब्ध करा रहा है।

ix. सरकार ने यह भी निर्देश दिया है कि सभी मंत्रालयों/विभागों और उनके संगठनों में आईसीटी अवसंरचना को सुरक्षित करने के लिए साइबर सुरक्षा के कार्यान्वयन हेतु अपने वार्षिक आईटी बजट की 10% धनराशि निर्धारित करें।

****