भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 1522

जिसका उत्तर 27 नवम्बर, 2019 को दिया जाना है।

6 अग्रहायण, 1941 (शक)

साइबर हमले

1522. श्री एस. वेंकटेशन:

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

(क) क्या हाल के दिनों में साइबर हमलों की घटनाएं बढ़ी हैं;

(ख) यदि हां, तो विगत तीन वर्षों में प्रत्येक वर्ष के दौरान सामने आए साइबर हमलों की घटनाओं सहित तत्संबंधी ब्यौरा क्या है और सरकार द्वारा इस संबंध में क्या कदम उठाए गए हैं; और

(ग) क्या ऐसे साइबर हमलों के पीछे विदेशी कंपनियों का हाथ है यदि हां, तो तत्संबंधी ब्यौरा क्या है तथा सरकार द्वारा इस संबंध में क्या प्रभावी कदम उठाए गए हैं और कार्रवाई की गई है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री संजय धोत्रे)

(क) और (ख) : भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को रिपोर्ट की गई और उसके द्वारा ट्रैक की गई सूचना के अनुसार फिशिंग, नेटवर्क स्कैनिंग और जांच पड़ताल, वायरस/विद्वेषपूर्ण कोड और वेबसाइट हैकिंग सहित वर्ष 2016, 2017, 2018 और 2019 (अक्टूबर तक) के दौरान क्रमश 50362, 53117, 208456 और 313649 साइबर सुरक्षा घटनाएं रिपोर्ट की गई।

सूचना प्रौद्योगिकी की गतिशील प्रकृति और उभरते हुए साइबर खतरों के अनुरूप, स्वामियों और उपयोगकर्ताओं द्वारा उचित सुरक्षा नियंत्रणों को सख्त कर और नियोजित कर नेटवर्क और डेटा को सुरक्षित रखने के लिए निरंतर प्रयास किए जाने की आवश्यकता है।

(i) भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) डिजिटल प्रौद्योगिकियों का सुरक्षित इस्तेमाल सुनिश्चित करने के लिए नियमित आधार पर नवीनतम साइबर खतरों/सुभेदताओं और प्रति उपाय के संबंध में चेतावनी और परामर्शी निदेश जारी करता है।

(ii) सरकार ने अनप्रयोगों/अवसंरचना की सुरक्षा और अनुपालन सुनिश्चित करने के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओएस) के लिए उनके महत्वपूर्ण भूमिका और जिम्मेदारियों के संबंध में दिशा-निर्देश जारी किए हैं।

(iii) सरकार ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन में सहायता देने और लेखापरीक्षा करने के लिए 90 साइबर सुरक्षा लेखापरीक्षा संगठनों को पैनलबद्ध किया है।

(iv) केन्द्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों/संघ राज्य क्षेत्रों 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।

(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 और अभ्यासों का संचालन किया जा रहा है। सर्ट-इन द्वारा अब तक ऐसे 44 अभ्यासों का संचालन किया गया है जहां वित्त, रक्षा, विद्युत, दूरसंचार, परिवहन, ऊर्जा, अंतरिक्ष आईटी/आईटीईएस इत्यादि जैसे क्षेत्रों और विभिन्न राज्यों से 265 संगठनों ने भाग लिया।

(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 प्रशिक्षण कार्यक्रम आयोजित करता है। 515 प्रतिभागियों सहित 19 प्रशिक्षण कार्यक्रम वर्ष 2019 अक्टूबर तक संचालित किए गए।

(vii) सरकार ने साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) स्थापित किया है। यह केंद्र मैलीशियस प्रोग्रामों का पता लगाने और उन्हें हटाने के लिए नि:शुल्क टूल उपलब्ध करा रहा है।

(viii) 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।

(ग) : भारतीय साइबर स्पेस पर साइबर हमले शुरू करने के लिए समय-समय पर प्रयास किए गए हैं। ऐसा देखा गया है कि अक्रमणकर्ता विश्व के विभिन्न भागों में स्थित कम्प्यूटर प्रणालियों के साथ छेड-छाड़ कर रहे हैं तथा वास्तविक प्रणालियों की पहचान को छिपाने के लिए छदम वेष तकनीक और अदृश्य सर्वरों का प्रयोग करते हैं ,जिनसे हमले किए जा रहे हैं। देश के बाहर ऐसी घटनाओं में शामिल प्रणालियों के समाधान के लिए सर्ट-इन बाहर के देशों में अपनी समकक्ष एजेसियों के साथ समन्वय स्थापित कर प्रतिउत्तर उपाय करता है।

****