भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 612

जिसका उत्तर 05 फरवरी, 2020 को दिया जाना है।

16 माघ, 1941 (शक)

साइबर हमले

612. श्री धैर्यशील संभाजीराव माणे:
डॉ. सुजय विखे पाटील:
श्री हेमन्त पाटिल:
श्री रंजीतसिन्हा हिंदूराव नाईक निम्बालकर:
श्री मन्नेश्रीनिवास रेड्डी:
डॉ. श्रीकांत एकनाथ शिंदे:

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

(क) क्या देश में साइबर हमलों की घटनाएं हाल के वर्षों में 2015 में 49,000 मामलों में 2017 में 53,000 मामलों और 2018 में 60,000 मामलों तक बढ़ गई है और यदि हां, तो तत्संबंधी ब्यौरा क्या है तथा चालू वित्त वर्ष में साइबर हमलों की राज्य/संघ राज्यक्षेत्र-वार कितनी घटनाएं दर्ज की गई हैं और इसके क्या कारण हैं;

(ख) सरकार द्वारा इस संबंध में क्या कार्रवाई की गई हैं;

(ग) क्या देश में साइबर हमलों की बहुत कम घटनाएं दर्ज होती हैं और इस बात को ध्यान में रखने पर इनकी वास्तविक संख्या और अधिक होगी और यदि हां, तो तत्संबंधी ब्यौरा क्या है और इसके क्या कारण हैं;

(घ) सरकार द्वारा इस संबंध में क्या कदम उठाए गए हैं;

(ङ) किन क्षेत्रों में साइबर हमलों की अधिक संभावनाएं हैं; और

(च) भारत पर मुख्य रूप से किन-किन प्रमुख देशों से साइबर हमले किए जाते हैं और उन्हें विफल करने के लिए मंत्रालय द्वारा कौन-से फायरवाल तैयार किए गए हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री संजय धोत्रे)

(क): साइबर स्पेस इंटरनेट पर व्यक्तियों, सॉफ्टवेयर, हार्डवेयर और सेवाओं का एक जटिल वातावरण है। सॉफ्टवेयर में सुभेद्यताओं, लोगों के बीच जागरूकता में कमी और उभरती प्रक्रियाओं के कारण साइबर सुरक्षा की घटनाओं में वृद्धि होने की संभावनाएं हैं। भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को रिपोर्ट की गई और उसके द्वारा ट्रैक की गई सूचना के अनुसार वर्ष 2015, 2016, 2017, 2018 और 2019 (अक्टूबर तक) के दौरान क्रमश: 49455, 50362, 53117, 208456 और 394499 साइबर सुरक्षा घटनाओं की रिपोर्ट की गई। राज्य/संघ राज्यक्षेत्र-वार डाटा केन्द्रीकृत रूप से नहीं रखा गया है।

(ख) : सूचना प्रौद्योगिकी की गतिशील प्रकृति और उभरते हुए साइबर खतरों के अनुरूप स्वामियों द्वारा उचित सुरक्षा नियंत्रणों को सख्त कर और नियोजित कर नेटवर्कों को सुरक्षित रखने के लिए निरंतर प्रयास किए जाने की आवश्यकता है।

सरकार ने देश ने देश में साइबर हमलों की घटनाओं को रोकने और साइबर सुरक्षा की स्थिति में सुधार करने के लिए निम्नलिखित उपाय किए है:

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

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

(iii) सभी सरकारी वेबसाइटों और एप्लीकेशनों को उनकी होस्टिंग के पहले साइबर सुरक्षा के संदर्भ में लेखापरीक्षित किया जाना है। होस्टिंग के बाद भी नियमित आधार पर वेबसाइटों और अनुप्रयोगों की लेखापरीक्षा की जाती है

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

(v) 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 और साइबर आंतकवाद से निपटने के लिए साइबर आपदा प्रबंधन योजना तैयार की है।

(vi) 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 अभ्यासों (मॉक ड्रिल) का संचालन किया जा रहा है। अब तक भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) द्वारा इस प्रकार के 44 अभ्यास संचालित किए हैं जिनमें विभिन्न राज्यों के वित्त, रक्षा, विद्युत, दूरसंचार, परिवहन, ऊर्जा, अंतरिक्ष आईटी/आईटीईएस इत्यादि क्षेत्रों से संबंधित 265 संगठनों के प्रतिभागियों ने भाग लिया।

(vii) 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। वर्ष 2019 में ऐसे तेइस (23) प्रशिक्षण कार्यक्रमों का आयोजन किया गया जिसमें 692 भागीदारों ने हिस्सा लिया।

(viii) सरकार ने साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग और 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।

(ix) 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) और (घ) : सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख और उनके तहत बनाए गए नियमों के अधीन सेवा प्रदाता, माध्यस्थों, डेटा केंद्रों और निगमित निकाय घटना घटित होने या नोटिस में आने के समय से उचित समय के भीतर सर्ट-इन को साइबर सुरक्षा घटनाओं की रिपोर्ट करेंगे जिससे कि उन पर समय पर कार्रवाई की जा सके। निम्न प्रकार की सुरक्षा घटनाएँ अनिवार्य रूप से सर्ट-इन को यथाशीघ्र सूचित की जाएगी ताकि इस पर कार्रवाई के लिए स्कोप छोड़ा जा सके : महत्वपूर्ण नेटवर्क/ प्रणालियों की लक्षित स्कैनिंग/जांच, महत्वपूर्ण प्रणालियों/सूचनाओं के साथ समझौता, सूचना प्रौद्योगिकी प्रणालियों/डेटा का अनाधिकृत अभिगम, वेबसाइट को विरूपित करना या वेबसाइट पर अनधिकार प्रवेश और अनधिकृत परिवर्तन जैसे विद्वेषपूर्ण कोड डालना, बाह्य वेबसाइटों के लिंक आदि, विद्वेषपूर्ण कोड हमला जैसे वायरस/वर्म/ट्रोजन/बोटनेट/स्पाइवेयर को फैलाना, सर्वर पर हमला जैसे डेटाबेस, मेल और डोमेन नाम प्रणाली और नेटवर्क डिवाइस जैसे: राउटर पहचान संबंधी चोरी, स्पूफिंग और फिशिंग अटैक, सेवा से मानाही ,सेवा हमलों से वितरित मानाही, महत्वपूर्ण अवसंरचनाओं, पर्यवेक्षी नियंत्रण और डेटा अधिग्रहण (एससीएडीए) प्रणालियों और वायरलेस नेटवर्क पर हमले, अनुप्रयोगों जैसे- ई-शासन, ई-कॉमर्स पर हमले आदि।

विभिन्न संगठनों और व्यक्तियों द्वारा सर्ट-इन को घटनाएं रिपोर्ट की जाती है। सर्ट-इन ने दिसम्बर, 2016 में अंग्रेजी और हिन्दी समाचार पत्रों में सुरक्षा घटनाओं की रिपोर्टिंग के संबंध में जागरूकता सृजन हेतु विज्ञापन प्रकाशित किए हैं। इसके अलावा, एमआईटीवाई और सर्ट-इन द्वारा आयोजित विभिन्न सेमिनारों/प्रशिक्षण कार्यक्रमों में साइबर सुरक्षा घटनाओं के विषय में नियमित रूप से सर्ट-इन को रिपोर्ट करने पर जोर दिया गया है।

(ङ): सूचना प्रौद्योगिकी और संबंधित सेवाओं के विस्तार के साथ देश के साथ-साथ वैश्विक स्तर पर साइबर सुरक्षा से संबंधित घटनाओं में वृद्धि हुई है। सर्ट-इन द्वारा रिपोर्ट की गई और ट्रैक की गई सूचना के अनुसार साइबर सुरक्षा से संबंधित घटनाएं अकादमिक, ई-वाणिज्य, ऊर्जा, मंनोरजन, वित्त, सरकार, स्वास्थ्य देखभाल, सूचना प्रौद्योगिकी, विनिर्माण, दूरसंचार, परिवहन इत्यादि क्षेत्रों में देखी गई है।

(च) : भारतीय साइबर स्पेस पर साइबर हमले शुरू करने के लिए समय-समय पर प्रयास किए गए हैं। ऐसा देखा गया है कि हमलावर विश्व के विभिन्न भागों में स्थित कम्प्यूटर प्रणालियों के साथ छेड-छाड़ कर रहे हैं तथा वास्तविक प्रणालियों, जिनसे हमले किए जा रहे की पहचान छिपाने के लिए छदम वेष तकनीक और अदृश्य सर्वरों का प्रयोग करते हैं। विश्लेषित किए गए और सर्ट-इन को उपलब्ध कराए गए लॉग के अनुसार ऐसी प्रतीत होता है कि कम्प्यूटरों, जहां से हमले किए गए हैं, के इन्टरनेट प्रोटोकॉल (आईपी) अड्रेस अलजीरिया, ब्राजील, चीन, फ्रांस, नीदरलैंड, उत्तरी कोरिया, पकिस्तान, रूस, सर्बिया, दक्षिण कोरिया, ताइवान, थाइलैंड, टूनिशिया, यूएसए, वियतनाम सहित विभिन्न देशों से संबंधित हैं।

****