भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 1879

जिसका उत्तर 3 जुलाई, 2019 को दिया जाना है।

12 आषाढ़, 1941 (शक)

साइबर हमले और साइबर आतंकवाद

1879. श्री राहुल रमेश शेवले :
श्री भर्तृहरि महताब :

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

(क) क्या दूरसंचार विभाग (डीओटी) ने भारतीय वाहकों पर साइबर हमलों और साइबर आतंकवाद को रोकने के लिए दिशानिर्देश जारी किए हैं और यदि हां, तो इन दिशानिर्देशों का ब्यौरा क्या है;

(ख) क्या सरकार ने गत तीन वर्षों में प्रत्येक वर्ष और चालू वर्ष के दौरान इन दिशानिर्देशों की समीक्षा की है और यदि हां, तो तत्संबंधी ब्यौरा और परिणाम क्या है;

(ग) क्या उक्त अवधि के दौरान विदेशों, विशेषकर चीन और पाकिस्तान से भारतीय वेबसाइटों पर साइबर हमलों और उनकी हैकिंग की घटनाएं बढ़ी हैं और यदि हां, तो तत्संबंधी देश-वार ब्यौरा क्या है; और

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

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री (श्री रवि शंकर प्रसाद)

(क) और (ख): दूर संचार विभाग ने मई/जून 2011 में अनुज्ञाप्ति करार के नियम व शर्तों में संशोधन के माध्यय से दूर संचार सेवा प्रदाताओं के लिए व्यापक सुरक्षा शर्तें जारी की हैं। तत्पश्चात इन्हें एकीकृत लाइसेंस के अभिन्न अंग के रूप में उपयुक्त बनाया गया है। इसकी मुख्य विशेषताएं निम्नानुसार हैं:-

(i) अनुज्ञाप्तिधारी अपने नेटवर्क की सुरक्षा के लिए पूर्णत: जिम्मेदार होगा।

(ii) अनुज्ञाप्तिधारी के पास नेटवर्क फॉरेंसिक्स, नेटवर्क सुदृढ़ता, नेटवर्क प्रवेश परीक्षण, जोखिम मूल्यांकन सहित अपने नेटवर्क की सुरक्षा और संरक्षा प्रबंधन पर संगठनात्मक नीति होगी।

(iii) अनुज्ञाप्तिधारी अपने नेटवर्क की लेखापरीक्षा करेगा या सुरक्षा के दृष्टिकोण से वर्ष में एक बार नेटवर्क लेखापरीक्षा करेगा अथवा प्रमाणन एजेंसी से नेटवर्क की लेखापरीक्षा करवाएगा।

(iv) अनुज्ञाप्तिधारी अपने दूरसंचार नेटवर्क में सिर्फ उन्हीं नेटवर्क अवयवों को प्रतिष्ठापित करेगा जिन्हें प्रसंगिक समकालीन भारतीय या अंतर्राष्ट्रीय सुरक्षा मानकों के अनुसार परीक्षित किया गया है।

(v) प्रमाणन सिर्फ प्राधिकृत और प्रमाणित एजेंसी/प्रयोगशालाओं से कराया जाएगा।

(vi) अनुज्ञाप्तिधारी सभी कंमांड लॉग का रिर्काड रखेगा।

(vii) अनुज्ञाप्तिधारी अपनी तकनीकी सुविधाओं पर होने वाले सभी प्रकार के घुसपैठ, हमला और धोखाधड़ी की निगरानी के लिए सुविधा बनाएगा और इसकी रिपोर्ट अनुज्ञाप्तिदाता/सर्ट-इन को देगा।

(ग) : 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। भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट इन) द्वारा ट्रैक की गई और इसे रिपोर्ट की गई सूचना के आनुसार, क्रमश: वर्ष 2016, 2017, 2018 और 2019 (मई तक) के दौरान कुल 33147, 30067,17560 और 10930 भारतीय वेबसाइट को हैक किया गया।

भारतीय साइबर स्पेस पर साइबर हमले शुरू करने के लिए समय-समय पर प्रयास किए गए हैं। ऐसा पाया गया है कि चीन और पाकिस्तान सहित कई देशों के साइबर स्पेस से हमले किए जाते हैं। यह देखा गया है कि हमलावर विश्व के विभिन्न भागों में स्थित कम्प्यूटर प्रणाली के साथ छेडछाड़ कर रहे हैं और वास्तविक प्रणाली की पहचान को छिपाने के लिए छद्म तकनीक और छिपे हुए सर्वर का उपयोग करते हैं जिनसे हमले शुरू किए जाते हैं।

(घ) : सरकार ने देश में साइबर सुरक्षा को बढ़ाने और साइबर सुरक्षा से संबंधित घटनाओं को रोकने के लिए अनेक कदम उठाए हैं। इनमें अन्य बातों के साथ-साथ निम्नलिखित उपाय 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।

ii. भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) नियमित आधार पर कंप्यूटर को सुरक्षित करने के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपाय के संबंध में चेतावनी और परामर्शी निदेश जारी करता है। प्रयोक्ताओं के अपने डेस्कटॉप और मोबाइल/स्मार्ट फोन की सुरक्षा को सक्षम बनाने के लिए सुरक्षा टिप्स प्रकाशित किए गए हैं।

iii. सरकार ने अनुप्रयोगों/अवसंरचना और अनुपालन 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।

iv. 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।

v. सरकार ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन में सहायता देने और लेखापरीक्षा करने के लिए 84 साइबर सुरक्षा लेखापरीक्षा संगठनों को पैनलबद्ध किया है।

vi. डिजिटल सेवा देने वाले सभी संगठनों को साइबर सुरक्षा से संबंधित घटनाओं के बारे में सर्ट-इन को शीघ्रता से रिपोर्ट करना अनिवार्य किया गया है।

vii. 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।

viii. 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 43 अभ्यास संचालित किए हैं जिनमें वित्त, रक्षा, विद्युत, दूरसंचार, परिवहन, ऊर्जा, अंतरिक्ष आईटी/आईटीईएस इत्यादि क्षेत्रों जैसे विभिन्न क्षेत्रों के प्रतिभागियों ने भाग लिया।

ix. 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 कम करने के लिए नियमित रूप से प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2018 में ऐसे 24 प्रशिक्षण कार्यक्रमों का आयोजन किया गया जिसमें 845 भागीदारों ने हिस्सा लिया।

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

xi. 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।

******