भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 3789
जिसका उत्तर 18 दिसंबर, 2024 को दिया जाना है।
27अग्रहायण, 1946 (शक)

राष्ट्रीय साइबर सुरक्षा नीति

3789.श्री इमरान मसूदः

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

(क) क्या देश के लिए व्यापक राष्ट्रीय साइबर सुरक्षा नीति का प्रारूप तैयार करने के लिए कोई कदम उठाए जा रहे हैं;
(ख) यदि हां, तो ऐसी रणनीति के प्रकाशन की अनुमानित तिथि सहित इसका ब्यौरा क्या है और यदि नहीं, तो इसकेक्या कारण हैं; और
(ग) क्या सरकार ने देश में साइबर सुरक्षा अवसंरचना और क्षमता निर्माण को बढ़ाने के लिए, अंतर्राष्ट्रीय साझीदारों और हितधारकों के साथ सहयोग सहित, कोई उपाय किए हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) और (ख): सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित और विश्वसनीय तथा उत्तरदायी इंटरनेट सुनिश्चित करना है। सरकार ने देश में साइबर सुरक्षा चुनौतियों से निपटने के लिए कई कानूनी, तकनीकी और प्रशासनिक नीतिगत प्रतिउपाय किए हैं। सरकार ने देश में साइबर सुरक्षा मामलों से निपटने के लिए एक राष्ट्रव्यापी एकीकृत और समन्वित प्रणाली को भी संस्थागत रूप दिया है, जिसमें अन्य बातों के साथ-साथ निम्नलिखित भीशामिल हैं:

(i) विभिन्न एजेंसियों के बीच समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) के अंतर्गत राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी) की स्थापना की गई है।

(ii) सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

(iii) सर्ट -इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। एनसीसीसी साइबर सुरक्षा खतरों को कम करने के लिए कार्रवाई करने हेतु साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

(iv) साइबर स्वच्छता केंद्र (सीएसके) सर्ट -इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है, जो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास भी प्रदान करता है।

(v) गृह मंत्रालय (एमएचए) ने साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) बनाया है।

(vi) सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70कके प्रावधानों के अंतर्गत, सरकार ने देश में महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है।

सुरक्षित और लचीले साइबरस्पेस को सुनिश्चित करने के लिए, प्राथमिक ध्यान तीन स्तंभों पर है: राष्ट्रीय साइबरस्पेस को सुरक्षित करना, लोगों, प्रक्रियाओं और क्षमताओं से युक्त मौजूदा संरचनाओं को सुदृढ़करना और देश में डिजिटल वातावरण की सुरक्षा के लिए उनके इष्टतम उपयोग हेतुसंसाधनों का समन्वय करना।

(ग):सरकार ने अंतर्राष्ट्रीय साझेदारों और हितधारकों के साथ सहयोग सहित देश में साइबर सुरक्षा अवसंरचना और क्षमता निर्माण को सुदृढ़ करने के लिए निम्नलिखित प्रतिउपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

(i) सर्ट -इन ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख की उप-धारा (6) के तहत साइबर सुरक्षा निर्देश जारी किए, जो सुरक्षित एवं विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा प्रथाओं, प्रक्रिया, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग से संबंधित हैं।

(ii) सर्ट -इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा लेखा परीक्षा जैसे डोमेन शामिल हैं।

(iii) सर्ट -इन ने सितंबर 2023 में सुरक्षित एप्लिकेशन डिजाइन, विकास और कार्यान्वयन और संचालन के लिए दिशानिर्देश जारी किए। सर्ट -इन ने अक्टूबर 2024 में संस्थाओं, विशेष रूप से सार्वजनिक क्षेत्र, सरकार, आवश्यक सेवाओं, सॉफ्टवेयर निर्यात और सॉफ्टवेयर सेवा उद्योग में शामिल संगठनों के लिए सॉफ्टवेयर बिल ऑफ मैटेरियल्स (एसबीओएम) दिशानिर्देश भी जारी किए हैं, ताकि संगठनों को यह जानने में मदद मिल सके कि उनके सॉफ्टवेयर या परिसंपत्तियों में कौन से घटक हैं, जिससे सुभेद्यताओं की पहचान करना और उन्हें ठीक करना आसान हो जाता है।

(iv) सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपायों के संबंध में निरंतर चुनौतियां और परामर्शी निदेश जारीकरता है।

(v) कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-वित्त क्षेत्र (सीएसआईआरटी-फिन) की स्थापना सर्ट - इन के तत्वावधान और मार्गदर्शन में वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने, उन्हें रोकने और शमन करने के लिए की गई है।

(vi) एनसीआईआईपीसी साइबर हमलों और साइबर आतंकवाद से बचाव के उपाय करने के लिए महत्वपूर्ण सूचना अवसंरचना (सीआईआईएस)/संरक्षित प्रणालियों (पीएस) वाले संगठनों को खतरे की आसूचना, स्थितिजन्य जागरूकता, चेतावनी और परामर्शी निदेश तथा सुभेद्यताओं के बारे में जानकारी प्रदान करता है।

(vii) सर्ट-इन एक स्वचालित साइबर खतरा आसूचना हेतु आदान-प्रदान मंच संचालित करता है, जो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ चेतावनियाँ एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है, ताकि वे सक्रिय रूप से खतरा न्यूनीकरण कार्रवाई कर सकें।

(viii) सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 155 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

(ix) सर्ट-इन अंतर्राष्ट्रीय सीईआरटी और सेवा प्रदाताओं के साथ घटना प्रतिक्रिया प्रतिउपायों का समन्वय करता है।

(x) साइबर सुरक्षा स्थिति और संगठनों की तैयारियों का आकलन करने तथा सरकारी और महत्वपूर्ण क्षेत्रों में लचीलापन बढ़ाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जाती हैं।

(xi) राष्ट्रीय सूचना विज्ञान केन्द्र (एनआईसी) ने सुभेद्यताओं को दूर करने और वैश्विक सुरक्षा मानकों के अनुपालन को सुनिश्चित करने तथा ऐसे अनुप्रयोगों को होस्ट करने वाले अंतर्निहित हार्डवेयर की सुभेद्यताका आकलन करने के लिए सर्ट-इन-सूचीबद्ध एजेंसियों के माध्यम से सरकारी वेबसाइटों और अनुप्रयोगों की आवधिक सुरक्षा लेखापरीक्षा अनिवार्य कर दी है।

(xii) सर्ट-इन कंप्यूटर सुरक्षा घटना प्रतिक्रिया दलों/विश्वसनीय परिचयकर्ता के लिए टास्क फोर्स का एक मान्यता प्राप्त सदस्य है। यह अन्य पक्षों को संकेत देता है कि सर्ट-इनपरिपक्वता और कार्यक्षमता के एक निश्चित स्तर पर पहुँच गया है, जो सर्ट समुदाय के भीतर विश्वास बनाने में मूल्यवान है। सर्ट-इन एशिया-प्रशांत क्षेत्र में इंटरनेट सुरक्षा के लिए एक क्षेत्रीय मंच, एशिया प्रशांत कंप्यूटर आपातकालीन प्रतिक्रिया दलों का एक परिचालन सदस्य है। सर्ट-इन फोरम ऑफ इंसिडेंट रिस्पांस एंड सिक्योरिटी टीम्स (फर्स्ट) का सदस्य है, जो साइबर सुरक्षा टीमों के लिए एक वैश्विक मंच है।

(xiii) साइबर सुरक्षा के क्षेत्र में सहयोग के लिए सर्ट-इन ने अपनी विदेशी समकक्ष एजेंसियों के साथ समझौता ज्ञापन (एमओयू) के रूप में सहयोग व्यवस्था की है। वर्तमान में बांग्लादेश, ब्राजील, मिस्र, एस्टोनिया, जापान, मालदीव, रूसी परिसंघ, यूनाइटेड किंगडम, उज्बेकिस्तान और वियतनाम के साथ ऐसे समझौता ज्ञापन (एमओयू) पर हस्ताक्षर किए गए हैं।

(xiv) सर्ट-इन सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों का शमन करने के बारे में नेटवर्क और सिस्टम प्रशासकों और सरकारी और महत्वपूर्ण क्षेत्र संगठनों के मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2024 (अक्टूबर तक) में 20 प्रशिक्षण कार्यक्रमों में कुल 9,807 अधिकारियों को प्रशिक्षित किया गया है।

(xv) एनआईसी विभिन्न ई-गवर्नेंस समाधानों के लिए केंद्र सरकार, राज्य सरकारों और जिला प्रशासकों के मंत्रालयों, विभागों और एजेंसियों को सूचना प्रौद्योगिकी (आईटी) सहायता प्रदान करता है और साइबर हमलों को रोकने और डेटा की सुरक्षा के उद्देश्य से उद्योग मानकों और प्रथाओं के अनुरूप सूचना सुरक्षा नीतियों और प्रथाओं का पालन करता है।

(xvi) साइबर सुरक्षा स्थिति और संगठनों की तैयारियों का आकलन करने तथा सरकारी और महत्वपूर्ण क्षेत्रों में लचीलापन बढ़ाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जा रही हैं। सर्ट-इन द्वारा अब तक 104 ऐसे अभ्यास आयोजित किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के 1420 संगठनों ने भाग लिया।

(xvii) एनआईसी ने सरकारी नेटवर्क से जुड़े सुरक्षा मुद्दों की पहचान करने के लिए खतरा आसूचना प्लेटफॉर्म सहित उन्नत सुरक्षा उपकरण नियोजित किए हैं।

(xviii) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। साइबर स्वच्छता और डीपफेक सहित साइबर सुरक्षा के विभिन्न पहलुओं पर हैंडबुक, लघु वीडियो, पोस्टर, ब्रोशर, बच्चों के लिए कार्टून कहानियां, परामर्शी निदेश आदि के रूप में जागरूकता सामग्री www.staysafeonline.in,www.infosecawareness.inऔर www.csk.gov.inजैसे पोर्टलों के माध्यम से प्रसारित की जाती है।

****