भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 4291

जिसका उत्तर 26 मार्च, 2025 को दिया जाना है।

05चैत्र, 1947 (शक)

साइबर सुरक्षा के खतरे और इससे निपटने के लिए राष्ट्रीय स्तर पर तैयारी

4291.एडवोकेट अदूर प्रकाश:

श्री बैन्नी बेहनन:

डॉ. धर्मवीर गांधी:

श्री के. सुधाकरन:

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

(क) वर्ष 2024 में महत्वपूर्ण अवसंरचना और सरकारी प्रणालियों को प्रभावित करने वाले साइबर सुरक्षा उल्लंघनों की संख्या कितनी है;

(ख) राष्ट्रीय साइबर सुरक्षा कार्यनीति के कार्यान्वयन सहित साइबर सुरक्षा की तैयारी को बढ़ाने के लिए क्या पहल की गई है; और

(ग) साइबर खतरों से निपटने के लिए निजी क्षेत्र की कंपनियों और अंतर्राष्ट्रीय भागीदारों के साथ सहयोग को सुदृढ़ करने के लिए क्या उपाय किए जा रहे हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क): सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए खुला, सुरक्षित और विश्वसनीय तथा उत्तरदायी इंटरनेट सुनिश्चित करना है। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) को साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के अंतर्गत राष्ट्रीय एजेंसी के रूप में नामित किया गया है। उल्लंघनों सहित साइबर सुरक्षा घटनाओं को देखते हुए, सर्ट-इन संबंधित संगठनों को उपचारात्मक उपाय सुझाता है।

सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") के अनुसार, महत्वपूर्ण सूचना अवसंरचना का अर्थ है ऐसा कंप्यूटर संसाधन जिसकी अक्षमता या विनाश का अन्य बातों के साथ-साथ राष्ट्रीय सुरक्षा पर भी बुरा प्रभाव पड़ता है। राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) को महत्वपूर्ण सूचना अवसंरचना संरक्षण के लिए आईटी अधिनियम की धारा 70क के प्रावधानों के अंतर्गत राष्ट्रीय नोडल एजेंसी के रूप में अधिसूचित किया गया है। एनसीआईआईपीसी ने सूचित किया है कि महत्वपूर्ण अवसंरचना पर साइबर सुरक्षा उल्लंघनों के बारे में विवरण प्रकट करना राष्ट्रीय सुरक्षा के हित में नहीं होगा।

(ख): सरकार ने देश में साइबर सुरक्षा तैयारियों को बढ़ाने के लिए निम्नलिखित पहल की हैं, जिनमें अन्य बातों के साथ-साथ शामिल हैं:

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

ii. 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 हेतु कार्रवाई करने के लिए साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

iii. 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 प्रोग्रामों का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है। यह नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और क्षेष्ठ पद्धतियां भी प्रदान करता है।

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

v. सर्ट-इन एक स्वचालित साइबर खतरा इंटेलिजेंस आदान-प्रदान मंच संचालित करता है, जो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है, ताकि वे सक्रिय रूप से खतरा न्यूनीकरण कार्रवाई कर सकें।

vi. सीईआरटी-इन ने साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है, जिसका कार्यान्वयन केंद्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों तथा महत्वपूर्ण क्षेत्रों द्वारा किया जाएगा।

vii. 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। सर्ट-इन द्वारा अब तक 109 ऐसे ड्रिल आयोजित किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के 1438 संगठनों ने भाग लिया।

viii. सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों और प्रतिउपायों के संबंध में निरंतर अलर्ट और परामर्श जारी करता है।

ix. सर्ट-इन ने सूचना सुरक्षा क्षेष्ठ पद्धतियों के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 200 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

x. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा पद्धतियों 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 ऑडिटिंग जैसे डोमेन शामिल हैं।

xi. 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 कमजोरियों की पहचान करना और उन्हें ठीक करना आसान हो जाता है।

xii. सर्ट-इन सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम 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। 2024 में 23 प्रशिक्षण कार्यक्रमों में कुल 12,014 अधिकारियों को प्रशिक्षित किया गया है।

xiii. सर्ट-इन नियमित रूप से साइबर हमलों और साइबर धोखाधड़ी के संबंध में जागरूकता और नागरिक संवेदीकरण के लिए विभिन्न गतिविधियों का आयोजन करता है।

xiv. 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, सलाह आदि के रूप में जागरूकता सामग्री www.staysafeonline.in, www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती है।

(ग): सरकार ने साइबर खतरों से निपटने के लिए निजी क्षेत्र की कंपनियों और अंतर्राष्ट्रीय साझेदारों तथा हितधारकों के साथ सहयोग को मजबूत करने के लिए निम्नलिखित उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं:

i. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) ने साइबर सुरक्षा की चुनौतियों से निपटने के लिए केंद्र/राज्य सरकारों, बैंकों और सार्वजनिक उपक्रमों के मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) और व्यापक आईटी समुदाय को शिक्षित और सक्षम बनाने के लिए सार्वजनिक निजी भागीदारी (पीपीपी) मोड में साइबर सुरक्षित भारत (सीएसबी) कार्यक्रम शुरू किया ।

ii. एमईआईटीवाई ने भारतीय डेटा सुरक्षा परिषद के सहयोग से साइबर सुरक्षा में राष्ट्रीय उत्कृष्टता केंद्र (एनसीओई) की स्थापना की है। एनसीओईका प्राथमिक उद्देश्य देश में साइबर सुरक्षा प्रौद्योगिकी विकास और उद्यमिता को उत्प्रेरित और गति प्रदान करने के लिए समन्वित प्रयास करना है।

iii. सर्ट-इन साइबर खतरे की सूचना के आदान-प्रदान, क्षेष्ठ पद्धतियों के विकास और क्षमता निर्माण के लिए उत्पाद और साइबर सुरक्षा कंपनियों के साथ सहयोग करता है। सर्ट-इन उद्योग भागीदारों के साथ मिलकर संयुक्त साइबर सुरक्षा प्रशिक्षण कार्यक्रम आयोजित करता है ताकि सरकारी, सार्वजनिक और निजी संगठनों में साइबर सुरक्षा कार्यबल को नवीनतम कौशल के साथ कुशल बनाया जा सके।

iv. सर्ट-इन, अंतर्राष्ट्रीय सीईआरटी और निजी क्षेत्र की कंपनियों सहित सेवा प्रदाताओं के साथ घटना प्रतिक्रिया उपायों पर सहयोग, कार्य और समन्वय करता है।

v. सर्ट-इन कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीमों / विश्वसनीय परिचयकर्ता के लिए टास्क फोर्स का एक मान्यता प्राप्त सदस्य है। सर्ट-इन एशिया प्रशांत कंप्यूटर आपातकालीन प्रतिक्रिया टीमों का एक परिचालन सदस्य है, जो एशिया-प्रशांत क्षेत्र में इंटरनेट सुरक्षा के लिए एक क्षेत्रीय मंच है। सर्ट-इन साइबर सुरक्षा टीमों के लिए एक वैश्विक मंच, फोरम ऑफ इंसीडेंट रिस्पॉन्स एंड सिक्योरिटी टीम्स (एफ़आईआरएसटी) का सदस्य है।

vi. 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, मिस्र, एस्टोनिया, जापान,

मालदीव, रूस, यूनाइटेड किंगडम और वियतनाम के साथ ऐसे समझौता ज्ञापन (एमओयू) पर हस्ताक्षर किए गए हैं।

****