भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2757

जिसका उत्तर 07 अगस्त, 2024 को दिया जाना है ।

16 श्रावण, 1946 (शक)

साइबर सुरक्षा संबंधी घटनाएं

2757. श्री के. सुधाकरन:
श्री सुखदेव भगत:
श्री सी. एम. रमेश:

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

(क) क्या 19 जुलाई, 2024 को विमानन, बैंकिंग, अस्पताल, प्रसारण आदि जैसे क्षेत्रों की विभिन्न सेवाओं में वैश्विक स्तर पर तकनीक के ठप्प होने के कारण आई रुकावट को देखते हुए सरकार की विंडोज ऑपरेटिंग सिस्टम और क्लाउड सेवाओं के साथ साइबर सुरक्षा सॉफ्टवेयर गठजोड़ विकसित करने की कोई योजना है और यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ख) क्या प्रणाली में उपरोक्त खराबी के कारण भारत में लगभग 500 उड़ानें रद्द/स्थगित कर दी गई थीं और मैनुअल प्रक्रियाओं का सहारा लिया गया था और यदि हां, तो देश में प्रभावित अन्य क्षेत्रों सहित तत्संबंधी ब्यौरा क्या है;

(ग) क्या सरकार को इस बात की जानकारी है कि सुरक्षा संबंधी घटना अथवा साइबर हमला हुआ है और रूस और चीन इस बड़ी बाधा से सुरक्षित हैं; और

(घ) क्या सरकार इन क्षेत्रों को उपकरणों की ऐसी खराबी और साइबर हमलों से बचाने के लिए अपनी स्वंय की विंडोज ऑपरेटिंग सिस्टम विकसित कर रही है और यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (घ): 19 जुलाई 2024 को भारतीय मानक समय के अनुसार सुबह लगभग 9.40 पर वैश्विक आउटेज देखा गया था। विभिन्न संगठनों में विंडोज कंप्यूटरों ने त्रुटि संदेश दिखाए और काम करना बंद कर दिया। विंडोज सिस्टम एक साइबर सुरक्षा भागीदार कंपनी द्वारा प्रदान किए गए साइबर खतरे का पता लगाने वाले समाधान पर दिए गए सॉफ़्टवेयर अपडेट के कारण बंद हुआ था। इस समस्या ने भारत सहित वैश्विक स्तर पर संगठनों और उपयोगकर्ताओं को प्रभावित किया जिसमें एयरलाइंस, विनिर्माण और आईटी क्षेत्र की सेवाएँ कुछ घंटों के लिए प्रभावित हुईं।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) ने आउटेज के संबंध में मेसर्स माइक्रोसॉफ्ट और इसकी साइबर सुरक्षा भागीदार कंपनी के साथ समन्वय किया। माइक्रोसॉफ्ट के साइबर सुरक्षा भागीदार ने इसे कंटेंट डिप्लॉयमेंट से संबंधित समस्या के रूप में पहचाना और परिवर्तनों को वापस ले लिया। सर्ट-इन ने 19 जुलाई 2024 को अपनी वेबसाइट पर एक एडवाइजरी प्रकाशित की जिसमें इस समस्या को ठीक करने के लिए उपचारात्मक उपाय बताए गए हैं। आउटेज से राष्ट्रीय सूचना विज्ञान केंद्र (एनआईएसी) और अन्य सरकारी प्रणालियों में से कोई भी प्रभावित नहीं हुआ।

सरकार ने निम्नलिखित समाधानों के विकास को समर्थन दिया है जिनमें अन्य बातों के साथ-साथ शामिल हैं:

i. मेघदूत क्लाउड सुइट एक व्यापक मुफ़्त और ओपन-सोर्स क्लाउड सुइट है। इसे ओपन स्टैक के साथ-साथ अन्य समाधानों और इन-हाउस डेवलपमेंट से तैयार किया गया है। यह क्लाउड सुइट पारंपरिक डेटा सेंटर को क्लाउड में बदल देता है जो इंफ्रास्ट्रक्चर ऐज़ ए सर्विस (आईएएएस), प्लेटफ़ॉर्म ऐज़ ए सर्विस (पीएएएस) और सॉफ़्टवेयर ऐज़ ए सर्विस (एसएएएस) की पेशकश करता है और साथ ही प्रबंधन और संचालन को आसान बनाता है। सुइट में प्लग एंड प्ले आर्किटेक्चर पर आधारित समाधान शामिल हैं और यह क्लाइंट की व्यावसायिक ज़रूरतों को पूरा करने के लिए अनुकूलन सुनिश्चित करता है। सुइट में क्लाउड संचालन और स्टैक के स्वचालित नियोजन के लिए एकीकृत डैशबोर्ड है। यह कई हाइपरवाइजर और विषम वातावरण का समर्थन करता है।

ii. भारत ऑपरेटिंग सिस्टम सॉल्यूशन (बीओएसएस) लिनक्स को सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग द्वारा विकसित किया गया है। बीओएसएस में एक उन्नत डेस्कटॉप वातावरण है जिसमें विभिन्न भारतीय भाषाओं और अनुदेशात्मक सॉफ़्टवेयर के लिए समर्थन शामिल है।

iii. सी-डैक ने मोबाइल ऑपरेटिंग सिस्टम का एक सुदृढ़ संस्करण विकसित किया है जो विशिष्ट कमर्शियल ऑफ-द-शेल्फ सॉफ्टवेयर (सीओटीएस) उपकरणों का समर्थन करता है। यह मोबाइल ऑपरेटिंग सिस्टम प्लेटफ़ॉर्म और कर्नेल परतों पर कस्टम सुरक्षा नीतियों का प्रवर्तन प्रदान करता है।

इसके अलावा, सभी उपयोगकर्ताओं को साइबर हमलों और मॉलवेयर हमलों से बचाने के लिए सरकार ने निम्नलिखित कदम उठाए हैं:

(i) सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के अंतर्गत 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।

(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) सर्ट-इन विभिन्न क्षेत्रों के संगठनों को लगभग वास्तविक समय में स्वचालित साइबर खतरे की खुफिया जानकारी प्रदान करता है ताकि वे खतरे को कम करने के लिए सक्रिय कार्रवाई कर सकें।

(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 मॉलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण प्रोग्रामों 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 श्रेष्ठ पद्धतियां भी प्रदान करता है।

(v) सर्ट-इन ने साइबर सुरक्षा ऑडिटिंग संगठनों को पैनल में शामिल किया है ताकि यह सुनिश्चित किया जा सके कि संगठनों में प्रयुक्त सूचना एवं संचार प्रौद्योगिकी (आईसीटी) प्रणालियां सुदृढ़ हों।

(vi) साइबर सुरक्षा स्थिति का आकलन करने और साइबर संकट की स्थितियों से निपटने के लिए सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारी को सक्षम करने के लिए सर्ट-इन द्वारा नियमित रूप से साइबर सुरक्षा मॉक ड्रिल और अभ्यास आयोजित किए जा रहे हैं।

(vii) सर्ट-इन प्रभावित संगठनों, अंतर्राष्ट्रीय सर्ट्स, विदेशी संगठनों, सेवा प्रदाताओं और कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों में सहयोग, कार्य और समन्वय करता है।

****