भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 2577
जिसका उत्तर 7 अगस्त, 2024 को दिया जाना है ।
16 श्रावण, 1946 (शक)

विश्व भर में विद्युत आपूर्ति का ठप्प होना

2577. श्री प्रभाकर रेड्डी वेमिरेड्डीः
श्री राजीव प्रताप रूडीः
श्री वसंतराव बलवंतराव चव्हाणः
श्री धैर्यशील संभाजीराव माणेः
श्री सुधीर गुप्ताः
प्रो. सौगत रायः

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

(क) क्या हाल ही में माइक्रोसॉफ्ट एज्योर के पूरी तरह ठप्प होने से सरकारी और अन्य प्राथमिक अंग, उड़ान सेवाओं और वित्तीय संभारतंत्रों सहित सार्वजनिक उपयोगिता सेवाएं प्रभावित हुई थीं;
(ख) यदि हां, तो देश की अर्थव्यवस्था पर पड़ने वाले प्रभावों सहित तत्संबंधी ब्यौरा क्या है और सरकार द्वारा स्थिति को पटरी पर लाने के लिए क्या उपाय किए गए हैं;
(ग) क्या सरकार को इस बात की जानकारी है कि इसका चीन और रूस पर कोई प्रभाव नहीं पड़ा है क्योंकि उनके अपने ऑपरेटिव सिस्टम हैं;
(घ) क्या भारत ने विश्व भर में लोगों की आवश्यकताओं को पूरा करने के लिए अपने सर्वर विकसित नहीं किए हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है;
(ङ) क्या माइक्रोसॉफ्ट एज्योर जैसे विदेशी सर्वरों पर निर्भरता देश की आंतरिक सुरक्षा को प्रभावित कर सकती है और यदि हां, तो तत्संबंधी ब्यौरा क्या है और इस संबंध में सरकार के अधीन कार्यरत भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया दल (आईसीईआरटी) की क्या भूमिका है; और
(च) क्या एनआईसी या सी-डैक इन विषयों पर कार्य कर रहा है या उन्होंने पहले कार्य किया है और यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

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

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) ने इस आउटेज के बारे 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 बदलावों को वापस ले लिया। सर्ट-इन ने 19 जुलाई 2024 को अपनी वेबसाइट पर एक एडवाइजरी प्रकाशित की है, जिसमें इस समस्या को ठीक करने के लिए उपचारात्मक उपाय बताए गए हैं।

माइक्रोसॉफ्ट सेवाओं में हाल ही में आई रुकावट का भारतीय रिजर्व बैंक (आरबीआई) की आईटी प्रणालियों और एप्लीकेशन्स पर कोई प्रभाव नहीं पड़ा। राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) के राष्ट्रीय डेटा केंद्र प्रभावित नहीं हुए।

सी-डैक ने उच्च-प्रदर्शन कंप्यूटिंग और क्लाउड के क्षेत्र में निम्नलिखित समाधानों को स्वदेशी रूप से डिजाइन और विकसित किया है:

(i) रूद्र बेस सर्वर: सी-डैक ने रूद्र-I सर्वर प्लेटफॉर्म को डिजाइन और विकसित किया है, जिसे उच्च-प्रदर्शन कंप्यूटिंग (एचपीसी), क्लाउड और एंटरप्राइज़ सर्वर बाजार की जरूरतों को पूरा करने के लिए कॉन्फ़िगर किया जा सकता है।

(ii) मेघदूत क्लाउड सूट: मेघदूत क्लाउड सूट एक व्यापक, निशुल्क और ओपन-सोर्स क्लाउड सूट है। यह क्लाउड सूट 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) ऑफरिंग का प्रावधान" करता है।

(iii) बॉस लिनक्स: सीडैक ने भारत ऑपरेटिंग सिस्टम सॉल्यूशन (बॉस) जारी किया है। बॉस एक कस्टमाइज्ड ऑपरेटिंग सिस्टम है जो ओपन-सोर्स जीएनयू/लिनक्स पर बनाया गया है और डेबियन ऑपरेटिंग सिस्टम पर आधारित है। यह बॉस https://www.bosslinux.in/ से मुफ्त डाउनलोड के लिए उपलब्ध है ।"

सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए खुली, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सुविधा उपल्बध कराना है। सरकार ने साइबर सुरक्षा स्थिति में सुधार करें और साइबर हमलों को रोकने के लिए निम्नलिखित उपाय किए हैं:

(i) सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर ज़ोखिमों/कमजोरियों और प्रतिउपायों के संबंध में निरंतर अलर्ट और सलाह जारी करता है।

(ii) सर्ट-इन फ़िशिंग वेबसाइटों को ट्रैक करने और उन्हें निष्क्रिय करने तथा धोखाधड़ी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों (एलईए) के साथ समन्वय में काम करता है।

(iii) सर्ट-इन ने विभिन्न मंत्रालयों को एक एड़वाइज़री जारी की है, जिसमें संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना का प्रसंस्करण करने वाली सभी संस्थाओं द्वारा साइबर सुरक्षा को मजबूत करने के लिए उठाए जाने वाले उपायों की रूपरेखा बताई गई है।

(iv) सर्ट-इन ने भारतीय रिजर्व बैंक के माध्यम से देश में प्रीपेड भुगतान उपकरण (वॉलेट) जारी करने वाली सभी अधिकृत संस्थाओं और बैंकों को सलाह दी है कि वे सर्ट-इन के पैनल में शामिल लेखा परीक्षकों से ऑडिट कराएं, ऑडिट रिपोर्ट में पहचाने गए गैर-अनुपालन को बंद करें और सुरक्षा संबंधी सर्वोत्तम प्रथाओं का कार्यान्वयन सुनिश्चित करें।

(v) सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम कार्यप्रणालियों के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 176 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

(vi) सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए हैं, जिनमें 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।

(vii) सर्ट-इन एक स्वचालित साइबर जोख़िम विनिमय प्लेटफार्म 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।

(viii) सर्ट-इन दुर्भावनापूर्ण प्रोग्रामों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र) संचालित करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है, साथ ही नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियां और सर्वोत्तम कार्यविधियाँ भी उपलब्ध कराता है।

(ix) सर्ट-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।

(x) सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा स्थिति और तैयारियों का आकलन करने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जा रही हैं। सर्ट-इन द्वारा अब तक 92 ऐसे अभ्यास आयोजित किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के लगभग 1,400 संगठनों ने भाग लिया।

(xi) सर्ट-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक स्थितिजन्य जागरूकता उत्पन्न करने के लिए राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) की स्थापना की है।

(xii) सर्ट-इन, वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने, उन्हें रोकने और कम करने के लिए अपने अधीन कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-वित्त क्षेत्र (सीएसआईआरटी-फिन) के संचालन के लिए नेतृत्व प्रदान करता है।

(xiii) सर्ट-इन नियमित रूप से साइबर सुरक्षा के केंद्रित विषयों पर सभी क्षेत्रों में स्टार्टअप और सूक्ष्म, लघु और मध्यम उद्यमों (एमएसएमई) सहित सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के तकनीकी कर्मचारियों को प्रशिक्षित करने के लिए प्रशिक्षण / कार्यशालाएँ आयोजित करता है। 2024 के दौरान, जून तक, सर्ट-इन ने सिस्टम/नेटवर्क प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) सहित 4,166 प्रतिभागियों को कवर करते हुए साइबर सुरक्षा के विभिन्न विशेष विषयों पर 9 प्रशिक्षण आयोजित किए हैं।

(xiv) उपयोगकर्ताओं के लिए अपने डेस्कटॉप और मोबाइल फोन को सुरक्षित रखने तथा फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की गई हैं।

(xv) सर्ट-इन नियमित रूप से साइबर हमलों और साइबर धोखाधड़ी के संबंध में जागरूकता और नागरिक संवेदनशीलता के लिए विभिन्न गतिविधियाँ आयोजित करता है।

(xvi) सर्ट-इन और भारतीय रिजर्व बैंक (आरबीआई) संयुक्त रूप से डिजिटल इंडिया प्लेटफॉर्म के माध्यम से "वित्तीय धोखाधड़ी से सावधान और जागरूक रहें", विषय पर साइबर सुरक्षा जागरूकता अभियान चला रहे हैं।

(xvii) इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में पुस्तकें, वीडियो और ऑनलाइन सामग्री आम उपयोगकर्ताओं, बच्चों और अभिभावकों के लिए विकसित की जाती है, और www.infosecawareness.in और www.csk.gov.in जैसे पोर्टल के माध्यम से प्रसारित की जाती हैं।

(xviii) दूरसंचार विभाग ने भारतीय दूरसंचार नेटवर्क के लिए संभावित साइबर जोख़िमों की निगरानी करने और उनका पता लगाने तथा आवश्यक कार्रवाई के लिए हितधारकों को समय पर अलर्ट प्रदान करने के लिए एक दूरसंचार सुरक्षा परिचालन केंद्र (टीएसओसी) की स्थापना की है।

****