भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या2644

जिसका उत्तर 11अगस्त, 2023 को दिया जाना है।

20श्रावण,1945(शक)

संवेदनशील और निजी डेटा में सेंधमारी

2644.श्री मल्लिकार्जुन खरगे:

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

(क)क्या सरकार साइबर सुरक्षा घटनाओं के मामलों जिसमें विशेषकर कोविन, एम्स, इपीएफओ और यूआईडीएआई डेटा में सेंधमारी, डेटा संबंधी हानि आदि हुई है और सरकार के अंतर्गत आने वाले विभाग, मंत्रालय अथवा संगठन प्रभावित हुए हैं, की सूची रखती है;

(ख)यदि हां, तो सुरक्षा संबंधी उन घटनाओं का ब्यौरा क्या है जिनसे डेटा की चोरी हुई है अथवा डेटा संबंधी हानि हुई है और ऐसे मामलों में सरकार द्वारा क्या कार्रवाई की गई; और

(ग)यदि नहीं, तो इसके क्या कारण हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) से (ग): जी, हाँ।

सरकार यह सुनिश्चित करने के लिए प्रतिबद्ध है कि भारत में इंटरनेट सभी उपयोगकर्ताओं के लिए सुरक्षित और विश्वसनीय और जवाबदेह हो। इंटरनेट के विस्तार और अधिक से अधिक भारतीयों के ऑनलाइन आने से साइबर घटनाओं की घटनाएं भी बढ़ी हैं। सरकार विभिन्न साइबर सुरक्षा खतरों से पूरी तरह परिचित और अवगत है। भारतीय कंप्यूटर आपात प्रतिक्रिया टीम (सर्ट-इन) डेटा उल्लंघनों और डेटा लीक के लिए जिम्मेदार साइबर सुरक्षा घटनाओं की एक सूची रखती है।

सर्ट-इन को दी गई और ट्रैक की गई जानकारी के अनुसार, वर्ष 2018, 2019, 2020, 2021, 2022 और 2023 (जून तक) के दौरान क्रमशः 0, 0, 14, 6, 27 और 15 डेटा लीक की घटनाएं और डेटा उल्लंघन की कुल 5, 11, 36, 39, 51 और 49 घटनाएं देखी गई हैं।

डेटा उल्लंघन/चोरी की घटनाएं आम तौर पर कई कारकों के संयोजन के कारण होती हैं, जिनमें संवेदनशील सेवाओं का दुरूपयोग, गलत कॉन्फ़िगरेशन, गलत क्रेडेंशियल्स, मैलवेयर संक्रमण और तृतीय-पक्ष उल्लंघन शामिल हैं।

सरकार ने साइबर सुरक्षा अवस्था को सुधारने और डेटा उल्लंघनों को रोकने के लिए निम्नलिखित उपाय किए हैं:

i. डेटा उल्लंघनों और डेटा लीक को देखने पर, सर्ट-इन प्रभावित संगठनों को उठाए जाने वाले उपचारात्मक कदमों के साथ सूचित करता है। सर्ट-इन प्रभावित संगठनों, सेवा प्रदाताओं, संबंधित क्षेत्र नियामकों के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।

ii. सर्ट-इन निरंतर आधार पर कंप्यूटर, नेटवर्क और डेटा की सुरक्षाके लिए नवीनतम साइबर खतरों/कमजोरियों और जवाबी उपायों के संबंध में अलर्ट और सलाह जारी करता है।

iii. दिसंबर 2022 में नवीनतम साइबर सुरक्षा खतरों के बारे में स्वास्थ्य क्षेत्र की संस्थाओं को संवेदनशील बनाने के लिए सर्ट-इन द्वारा स्वास्थ्य क्षेत्र की संस्थाओं का लचीलापन बढ़ाने हेतु सुरक्षा पद्धतियों पर एक विशेष सलाह स्वास्थ्य और परिवार कल्याण मंत्रालय को भेजी गई है। मंत्रालय से अनुरोध किया गया है कि वह देश में सभी प्राधिकृत चिकित्सा परिचर्या संस्थाओं/सेवा प्रदाताओं के बीच इन परामर्शी निदेशों का प्रसार करे।

iv. सर्ट-इन एक स्वचालित साइबर थ्रेट एक्सचेंज प्लेटफॉर्म संचालित करता है, जो विभिन्न क्षेत्रों के संगठनों के साथ उनके द्वारा सक्रिय खतरे को कम करने हेतु अलर्ट एकत्र करने, विश्लेषण करने और साझा करने के लिए है।

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

vi. सर्ट –इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए हैं, 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।

vii. सरकार ने केंद्र सरकार, राज्य सरकारों और उनके संगठनों और महत्वपूर्ण क्षेत्रों के सभी मंत्रालयों/विभागों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है।

*****