भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 1381
जिसका उत्तर 31 जुलाई, 2024 को दिया जाना है।
9 श्रावण, 1946 (शक)

सिंगापुर स्थित साइबर सुरक्षा कंपनी

1381. श्री बालाशौरी वल्लभनेनीः

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

(क) क्या सरकार को सिंगापुर स्थित साइबर सुरक्षा फर्म साइफर्मा रिपोर्ट की 'इंडियन थ्रेट लैंडस्केप रिपोर्ट' की जानकारी है जिसमें यह दर्शाया गया है कि वर्ष 2021 और सितम्बर, 2023 के बीच तीन वर्षों में देश पर राज्य प्रायोजित साइबर हमलों में लगभग 300 प्रतिशत की वृद्धि हुई है;

(ख) क्या यह भी सच है कि सेवा क्षेत्र की कंपनियों, बिजनेस प्रोसेस आउटसोर्सिंग पर सर्वाधिक हमले हुए हैं;

(ग) क्या यह भी सच है कि सरकारी एजेंसियों पर लक्षित साइबर हमलों में 460 प्रतिशत की वृद्धि हुई है और स्टार्ट-अप्स तथा एमएसएमई पर 500 प्रतिशत की वृद्धि हुई है; और

(घ) क्या सरकार इसे रोकने और हमारे साइबर स्पेस की सुरक्षा करने की योजना बना रही है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (घ) सरकार ने साइबर सुरक्षा की स्थिति में सुधार करने और साइबर हमलों को रोकने के लिए निम्नलिखित उपाय किए हैः-

i. सर्ट-इन नवीनतम साइबर जोखिमों/कमियों के संबंध में चेतावनियां और सलाह जारी करता है तथा कम्प्यूटरों, मोबाइल फोनों, नेटवर्कों और आंकड़ों की सतत आधार पर सुरक्षा करने के लिए प्रत्युपाय करता है।
ii. सर्ट-इन फिशिंग वेबसाइटों को ट्रैक और अक्षम करने और धोखाधड़ी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों (एलईए) के साथ समन्वय का काम करता है।
iii. सर्ट-इन ने विभिन्न मंत्रालयों को एक एडवाइजरी जारी की है जिसमें साइबर सुरक्षा को सुदृढ़ करने के लिए उन सभी संस्थाओं द्वारा किए जाने वाले उपायों की रूपरेखा दी गई है जो संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना को संसाधित कर रहे हैं।
iv. सर्ट-इन ने आरबीआई के माध्यम से देश में प्री-पेड भुगतान लिखत (वॉलेट) जारी करने वाली सभी प्राधिकृत कंपनियों और बैंकों को सर्ट-इन-पैनलबद्ध लेखा परीक्षकों द्वारा विशेष लेखा परीक्षा करने, लेखा परीक्षा रिपोर्ट में पहचाने गए गैर-अनुपालन को बंद करने और सुरक्षा सर्वोत्तम प्रथाओं का कार्यान्वयन सुनिश्चित करने की सलाह दी है।

v. सर्ट-इन ने सूचना सुरक्षा संबंधी सर्वोत्तम पद्धतियों के कार्यान्वयन में मदद करने और लेखा परीक्षा करने के लिए 176 सुरक्षा लेखा परीक्षा संगठनों को सूचीबद्ध किया है।

vi. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा पद्धतियों पर दिशानिर्देश जारी किए हैं, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, थर्ड पार्टी आउटसोर्सिंग, हार्डनिंग प्रोसीजर्स, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा लेखा परीक्षा जैसे डोमेन शामिल हैं।

vii. सर्ट-इन खतरों को सक्रियतापूर्वक कम करने के लिए सभी क्षेत्रों में संगठनों के साथ अलर्ट एकत्र करने, विश्लेषण करने और उसे साझा करने के लिए एक स्वचालित साइबर जोखिम विनिमय प्लेटफार्म का संचालन करता है।

viii. सर्ट-इन दुर्भावनापूर्ण कार्यक्रमों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) संचालित करता है और इसे हटाने के लिए निःशुल्क उपकरण प्रदान करता है तथा नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम कार्यविधियाँ भी उपलब्ध कराता है।

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

x. साइबर सुरक्षा की स्थिति और सरकारी एवं महत्वपूर्ण क्षेत्रों के संगठनों की तैयारी का आकलन करने के लिए नियमित रूप से साइबर सुरक्षा मॉक ड्रिल आयोजित की जा रही है। सर्ट-इन द्वारा अब तक 92 ऐसे ड्रिल्स 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 जोखिमों के बारे में आवश्यक स्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) की स्थापना की है।

xii. सर्ट-इन वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं का जवाब देने और नियंत्रित करने और कम करने के लिए अपनी निगरानी में कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीम-वित्त क्षेत्र (सीएसआईआरटी-फिन) के संचालन के लिए नेतृत्व प्रदान करता है।

xiii. सर्ट-इन साइबर सुरक्षा केन्द्रित विषयों पर सभी क्षेत्रों में स्टार्टअप्स और सूक्ष्म, लघु और मध्यम उद्यमों (एमएसएमई) सहित सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के तकनीकी कर्मचारियों को प्रशिक्षित करने के लिए नियमित रूप से प्रशिक्षण/ कार्यशालाएं आयोजित करता है। वर्ष 2024 के दौरान, जून तक सर्ट-इन ने साइबर सुरक्षा के विभिन्न विशिष्ट विषयों पर 9 प्रशिक्षण आयोजित किए हैं, जिनमें सिस्टम/नेटवर्क प्रशासक और मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) सहित 4,166 प्रतिभागी शामिल हुए हैं।

xiv. उपयोगकर्ताओं को अपने डेस्कटॉप और मोबाइल फोन को सुरक्षित करने और फ़िशिंग हमलों को रोकने में सहायता करने 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 संवेदीकरण के लिए विभिन्न गतिविधियां आयोजित करता है।

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

xvii. इलेक्ट्रॉनिकी 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 सामान्य उपयोगकर्ताओं, बच्चों और माता-पिता के लिए तैयार की जाती हैं और www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती हैं।

xviii. दूरसंचार विभाग ने भारतीय दूरसंचार नेटवर्क के लिए संभावित साइबर जोखिमों की निगरानी करने और उनका पता लगाने तथा आवश्यक कार्रवाई हेतु स्टेकहोल्डरों को समय पर अलर्ट प्रदान करने हेतु दूरसंचार सुरक्षा प्रचालन केन्द्र (टीएसओसी) की स्थापना की है।

****