भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 1635

जिसका उत्तर 29 जुलाई, 2026 को दिया जाना है।

7 श्रावण, 1948 (शक)

सरकारी डिजिटल प्लेटफ़ॉर्म पर डेटा की सेंधमारी

1635. श्री सु. वेंकटेशनः

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

(क) पिछले वर्ष सरकारी डिजिटल प्लेटफ़ॉर्म पर डेटा की सेंधमारी की घटनाओं की रिपोर्ट किए जाने या इनके संज्ञान में आने की संख्या कितनी है;
(ख) सरकार द्वारा हाल की साइबर सुरक्षा संपरीक्षा में सामने आई कमियों को दूर करने के लिए उठाए गए विशेष सुधारात्मक कदमों का ब्यौरा क्या है; और
(ग) सरकार द्वारा विधि प्रवर्तक अभिकरणों के साथ नागरिकों का डेटा साझा करते समय अपनाए जाने वाले विधिक नयाचार और मानक संचालन प्रक्रिया (एसओपी) का ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से **(ग):** सरकार एक खुला, सुरक्षित, विश्वसनीय और जवाबदेह साइबर स्पेस सुनिश्चित करने के लिए प्रतिबद्ध है। देश में साइबर सुरक्षा चुनौतियों से निपटने के लिए कई कानूनी, तकनीकी और प्रशासनिक नीतिगत उपाय लागू किए गए हैं।

सरकार ने देश में साइबर हमलों से निपटने के लिए एक राष्ट्रव्यापी एकीकृत और समन्वित प्रणाली को संस्थागत रूप दिया है जिसमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं -

i. **भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को** सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत साइबर सुरक्षा घटनाओं पर कार्रवाई करने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

ii. सर्ट-इन ने ऑडिटिंग के लिए 'सूचना सुरक्षा लेखा परीक्षा संगठनों' का एक पैनल बनाया है, जिसमें कंप्यूटर सिस्टम, नेटवर्क, वेबसाइटों और सरकार के विभिन्न संगठनों और महत्वपूर्ण क्षेत्रों के अनुप्रयोगों की भेद्यता मूल्यांकन और प्रसार परीक्षण शामिल है। सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन का समर्थन और लेखा परीक्षा करने के लिए 237 सूचना सुरक्षा लेखा परीक्षा संगठनों को सर्ट-इन द्वारा सूचीबद्ध किया गया है।

iii. प्रारंभिक ऑडिट के दौरान पैनल में शामिल संगठनों द्वारा पहचानी गई कमजोरियों का संबंधित संस्थाओं द्वारा उचित समाधान उपायों के माध्यम से समाधान किया जाता है, जिसमें पैचिंग और शमन शामिल हैं।

इसके बाद, ऑडिटिंग संगठन पहचानी गई कमजोरियों को प्रभावी ढंग से बंद करने और निर्धारित साइबर सुरक्षा आवश्यकताओं और सिफारिशों के अनुपालन का आकलन करने के लिए पुनर्वैधीकरण लेखा परीक्षा करते हैं।

iv.सर्ट-इन ने महत्वपूर्ण बुनियादी ढांचे सहित सभी क्षेत्रों में सुसंगत, प्रभावी और सुरक्षित तरीके से साइबर सुरक्षा ऑडिट करने की रणनीति के साथ "व्यापक साइबर सुरक्षा ऑडिट नीति दिशानिर्देश" विकसित और जारी किए हैं।

सर्ट-इन प्रभावित संगठनों, सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।

vi.सर्ट-इन **द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी),** साइबर सुरक्षा खतरों का पता लगाने के लिए साइबरस्पेस की जांच करता है। यह कार्रवाई करने के लिए संबंधित संगठनों, राज्य सरकारों और हितधारक एजेंसियों के साथ जानकारी साझा करता है।

vii.सर्ट-इन सक्रिय खतरे को कम करने के लिए विभिन्न क्षेत्रों के संगठनों के साथ अनुरूप अलर्ट साझा करने के लिए एक स्वचालित साइबर थ्रेट इंटेलिजेंस एक्सचेंज प्लेटफॉर्म संचालित करता है।

viii. **साइबर स्वच्छता केंद्र (सीएसके)**

● सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा, जो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करती है।

● यह बॉटनेट क्लीनिंग एंड मैलवेयर एनालिसिस सेंटर है और दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और इसे हटाने के लिए मुफ्त टूल प्रदान करता है।

● यह नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और श्रेष्ठ पद्धतियाँ भी प्रदान करता है।

ix. **सेक्टोरल कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल (सीएसआईआरटी)**

● बैंकिंग और वित्तीय क्षेत्र में साइबर घटना प्रतिक्रिया के समन्वय के लिए सर्ट-इन के तहत वित्त क्षेत्र में सीएसआईआरटी (सीएसआईआरटी-फाइन) मई 2020 से चालू है।

● सीएसआईआरटी-पावर सितंबर 2024 से बिजली क्षेत्र की संस्थाओं के भीतर साइबर सुरक्षा के मुद्दों के समन्वय के लिए सर्ट-इन एक विस्तारित शाखा के रूप में काम कर रहा है।

(x) सर्ट-इन ने सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना (सीसीएमपी) तैयार की है।

xi.साइबर सुरक्षा मॉक ड्रिल सर्ट-इन द्वारा नियमित रूप से आयोजित किए जाते हैं, ताकि साइबर सुरक्षा स्थिति और सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारियों का आकलनकिया जा सके।xii. सर्ट-इन ने सॉफ्टवेयर/उपकरणों में कमजोरियों को ठीक करने के लिए शोधकर्ताओं/अन्वेषकों/विक्रेताओं के साथ

संग्रह, विश्लेषण, शमन और समन्वय के लिए एक जिम्मेदार भेद्यता प्रकटीकरण और समन्वय कार्यक्रम का संचालन किया है।

xiii. सर्ट-इन कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों और प्रतिउपायों के बारे में अलर्ट और परामर्शी निदेश जारी करता है।

xiv. सर्ट-इन सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के आईटी/साइबर सुरक्षा पेशेवरों के लिए नियमित साइबर सुरक्षा प्रशिक्षण, कार्यशालाएं आयोजित करता है।

xv. **डिजिटल वैयक्तिक डेटा संरक्षण अधिनियम, 2023 के तहत प्रावधान**

- सरकार ने डिजिटल वैयक्तिक डेटा संरक्षण अधिनियम, 2023 और उसके तहत बनाए गए नियमों के तहत एक वैधानिक ढांचा स्थापित किया है ताकि यह सुनिश्चित किया जा सके कि कानून प्रवर्तन उद्देश्यों के लिए नागरिकों के डिजिटल व्यक्तिगत डेटा को साझा करना और संसाधित करना कानूनी, सुरक्षित और जवाबदेह तरीके से किया जाए।
- यह अधिनियम ऐसे व्यक्तिगत डेटा को प्राप्त करने के लिए कानून द्वारा अधिकृत किसी अन्य डेटा न्यासीय के साथ व्यक्तिगत डेटा साझा करने को मान्यता देता है, जहां साझा करना अपराधों या साइबर घटनाओं की रोकथाम,उनका पता लगाने या जांच, या अपराधों के अभियोजन या सजा के लिए लिखित रूप में किए गए अनुरोध के अनुसार होता है। इसके अलावा इसमें प्रसंस्करण का भी प्रावधान है जिसके तहत किसी भी अपराध की रोकथाम, पता लगाने, जांच या अभियोजन के हित में या भारत में किसी भी कानून के उल्लंघन पर व्यक्तिगत डेटा को संसाधित किया जाता है।
- डिजिटल पर्सनल डेटा प्रोटेक्शन रूल्स, 2025 में सुरक्षा के उचित उपाय बताए गए हैं। इनमें शामिल हैं: एन्क्रिप्शन, अस्पष्टीकरण, मास्किंग या वर्चुअल टोकन के इस्तेमाल से पर्सनल डेटा को सुरक्षित करना; अनधिकृत एक्सेस का पता लगाने के लिए उचित उपाय; तय समय तक लॉग और अन्य ज़रूरी डेटा को संभालकर रखना; डेटा प्रोसेसर के शामिल होने पर उचित कॉन्ट्रैक्ट प्रावधान; और सुरक्षा उपायों का प्रभावी ढंग से पालन सुनिश्चित करने के लिए उचित तकनीकी और संगठनात्मक उपाय।
- तदनुसार, अधिनियम और नियमों के तहत ढांचा यह सुनिश्चित करता है कि कानून प्रवर्तन एजेंसियों के साथ नागरिकों के व्यक्तिगत डेटा को प्रलेखित प्रक्रियाओं के माध्यम से वैध प्राधिकार के अनुसार साझा किया जाता है और उचित सुरक्षा सुरक्षा उपायों और संस्थागत जवाबदेही के बशर्ते किया जाता है।

****