भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2761

जिसका उत्तर 05 अगस्त, 2026 को दिया जाना है।

14 श्रावण, 1948 (शक)

साइबर हमलों की घटनाएं

2761. श्री नारायण तातू राणेः
श्री संजय उत्तमराव देशमुखः
श्रीमती मंजू शर्माः
श्री संजय हरिभाऊ जाधवः

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

(क) वर्ष 2022 से आज तक देश में सरकारी वेबसाइटों, डिजिटल प्लेटफॉर्मों और महत्वपूर्ण अवसंरचना पर साइबर हमलों की घटनाओं की संख्या कितनी है;

(ख) उक्त साइबर हमलों के प्रकार और ब्यौरा क्या है;

(ग) उक्त साइबर हमलों के ऐसे मामलों की संख्या कितनी है जिनमें संवेदनशील डेटा से समझौता हुआ था तथा अपराधियों के विरुद्ध विशेष रूप से महाराष्ट्र में की गई कार्रवाई का ब्यौरा क्या है;

(घ) क्या सरकार विशेष रूप से हालिया सुरक्षा उल्लंघनों के आलोक में साइबर हमलों की बढ़ती संख्या से निपटने के लिए मौजूदा कानूनी ढांचे को पर्याप्त मानती है और यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ङ) क्या सरकार का बढ़ते साइबर हमलों के विरुद्ध उन्नत सुरक्षा प्रदान करने के लिए आवश्यक अवसंरचना स्थापित करने का विचार है और यदि हां, तो भविष्य में ऐसी घटनाओं को रोकने के लिए ऐसी योजनाएं तैयार करने हेतु सरकार द्वारा किए गए उपायों का ब्यौरा क्या है;

(च) व्यक्तिगत डिजिटल डेटा की सुरक्षा सुनिश्चित करने के लिए सरकार द्वारा उठाए गए प्रमुख कदम क्या हैं; और

(छ) डेटा संरक्षण से संबंधित नियमों के कार्यान्वयन की वर्तमान स्थिति क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री
(श्री जितिन प्रसाद)

(क) से (छ): 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।

भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सीईआरटी-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। सर्ट-इन द्वारा प्राप्त और ट्रैक की गई जानकारी के अनुसार, वर्ष 2022 से अब तक केंद्रीय मंत्रालयों/विभागों और राज्य सरकारों (महाराष्ट्र सहित) से संबंधित साइबर सुरक्षा घटनाओं की कुल संख्या नीचे दी गई है:

वर्ष	संख्या
2022	192439
2023	204844
2024	1309372
2025	1821767
2026 (जून तक)	1075220

सरकारी-प्रबंधित प्लेटफार्मों से संबंधित घटनाओं सहित साइबर सुरक्षा घटनाओं को देखते हुए, सर्ट-इन प्रभावित संगठनों, सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।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. विभिन्न एजेंसियों के बीच साइबर सुरक्षा से संबंधित समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) के तहत **राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी)** की स्थापना की गई है।

ii. 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।

iii. **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।

iv. **सेक्टोरल कंप्यूटर सिक्योरिटी इंसिडेंट रिस्पांस टीम (सीएसआईआरटी)**

- बैंकिंग और वित्तीय क्षेत्र में साइबर घटना प्रतिक्रिया के समन्वय के लिए सर्ट-इन के तहत वित्त क्षेत्र में सीएसआईआरटी (सीएसआईआरटी-फिन) मई 2020 से चालू है।
- सीएसआईआरटी-पावर सितंबर 2024 से बिजली क्षेत्र की संस्थाओं के भीतर साइबर सुरक्षा मुद्दों के समन्वय के लिए सर्ट-इन की एक विस्तारित शाखा के रूप में चालू है।

v. सर्ट-इन एक स्वचालित साइबर खतरे की खुफिया जानकारी साझा करने वाला मंच संचालित करता है, जिसका उपयोग विभिन्न क्षेत्रों के संगठनों के साथ अनुकूलित अलर्ट साझा करने और खतरों को पहले से ही कम करने के लिए किया जाता है।

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

vii.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" तैयार और जारी किए हैं।

viii.सर्ट-इन ने सरकारी और महत्वपूर्ण क्षेत्रों के विभिन्न संगठनों के कंप्यूटर सिस्टम, नेटवर्क, वेबसाइट और एप्लिकेशन की सुरक्षा संबंधी कमजोरियों का आकलन और पैठ परीक्षण सहित ऑडिट करने के लिए 'सूचना सुरक्षा ऑडिटिंग संगठनों' का एक पैनल बनाया है। सूचना सुरक्षा संबंधी श्रेष्ठ पद्धतियों के कार्यान्वयन में सहयोग और ऑडिट करने के लिए सर्ट-इन द्वारा 237 सूचना सुरक्षा लेखापरीक्षण संगठनों को सूचीबद्ध किया गया है।

ix. सभी सरकारी वेबसाइटों और एप्लीकेशनों को उनकी होस्टिंग से पहले साइबर सुरक्षा के सन्दर्भ में ऑडिट किया जाता है। वेबसाइटों और अनुप्रयोगों की ऑडिटिंग होस्टिंग के बाद भी नियमित आधार पर की जाती है।

x. सर्ट-इन ने सॉफ्टवेयर/उपकरणों में मौजूद कमजोरियों को दूर करने के लिए शोधकर्ताओं/खोजकर्ताओं/विक्रेताओं के साथ समन्वय, विश्लेषण और जानकारी एकत्र करने हेतु एक जिम्मेदार भेद्यता प्रकटीकरण और समन्वय कार्यक्रम को क्रियान्वित किया 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 आकलन किया जा सके।

xii. 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।

xiii. सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के तहत देश में महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा के लिए **राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी)** की स्थापना की गई है।

xiv. एनसीआईआईपीसी वास्तविक समय के खतरे की खुफिया जानकारी और स्थितिजन्य जागरूकता प्रदान करता है जिसके आधार पर क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर (सीआईआई)/प्रोटेक्टेड सिस्टम (पीएस) संस्थाओं को नियमित अलर्ट और परामर्शी निदेश भेजे जाते हैं।

xv. एनसीआईआईपीसी समय-समय पर महत्वपूर्ण सूचना अवसंरचना/संरक्षित प्रणालियों की कमजोरियों और जोखिम का मूल्यांकन करता है और सभी संबंधितों को प्रतिक्रिया देता है।

xvi. डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 के तहत प्रावधान

- सरकार ने डिजिटल व्यक्तिगत 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 व्यक्तिगत डेटा को किसी अन्य डेटा फिड्यूशरी के साथ साझा करने की अनुमति देता है, जिसे कानून द्वारा ऐसा व्यक्तिगत डेटा प्राप्त करने के लिए अधिकृत किया गया है, जहां यह साझाकरण अपराधों या साइबर घटनाओं की रोकथाम, पता लगाने या जांच करने, या अपराधों के अभियोजन या दंड के लिए लिखित अनुरोध के अनुसार किया जाता है। यह आगे उन मामलों में भी व्यक्तिगत डेटा के प्रसंस्करण का प्रावधान करता है जहां व्यक्तिगत डेटा को भारत में लागू किसी भी कानून के उल्लंघन या किसी भी अपराध की रोकथाम, पता लगाने, जांच या अभियोजन के हित में संसाधित किया जाता है।
- डिजिटल व्यक्तिगत डेटा संरक्षण नियम, 2025 में उचित सुरक्षा उपायों का प्रावधान है, जिसमें एन्क्रिप्शन, अस्पष्टीकरण, मास्किंग या वर्चुअल टोकन के उपयोग के माध्यम से व्यक्तिगत डेटा को सुरक्षित करना, अनधिकृत पहुंच का पता लगाने के लिए उचित उपाय, निर्धारित अवधि के लिए लॉग और अन्य प्रासंगिक डेटा का प्रतिधारण, जहां डेटा प्रोसेसर नियुक्त किया गया है वहां उपयुक्त संविदात्मक प्रावधान, और सुरक्षा उपायों के प्रभावी अनुपालन को सुनिश्चित करने के लिए उपयुक्त तकनीकी और संगठनात्मक उपाय शामिल हैं।
- तदनुसार, अधिनियम और नियमों के अंतर्गत ढांचा यह सुनिश्चित करता है कि कानून प्रवर्तन एजेंसियों के साथ नागरिकों के व्यक्तिगत डेटा को साझा करना वैध अधिकार के अनुसार, दस्तावेजी प्रक्रियाओं के माध्यम से और उचित सुरक्षा उपायों और संस्थागत जवाबदेही के अधीन किया जाता है।
- डीपीडीपी नियम चरणों में लागू किए जाते हैं:
    i. नियम 1, 2 और 17 से 21 नवंबर 2025 में आधिकारिक राजपत्र में प्रकाशन के बाद लागू हुए। इन प्रावधानों में नियमों के शीर्षक और परिभाषाओं और डेटा संरक्षण बोर्ड की नियुक्ति, सेवा शर्तों, कामकाज और प्रशासन से संबंधित मामले शामिल हैं।
    ii. सहमति प्रबंधकों के पंजीकरण और दायित्वों से संबंधित नियम 4, प्रकाशन के एक साल बाद, नवंबर 2026 में लागू होने वाला है।
    iii. नियम 3, 5 से 16, 22 और 23 प्रकाशन के अठारह महीने बाद, मई 2027 में लागू होने वाले हैं। इनमें नोटिस, उचित सुरक्षा उपाय, व्यक्तिगत डेटा उल्लंघन रिपोर्टिंग, डेटा प्रतिधारण, बच्चों के डेटा, महत्वपूर्ण डेटा न्यासियों और डेटा प्रिंसिपल अधिकारों के प्रयोग से संबंधित प्रावधान शामिल हैं।

****