भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2823

जिसका उत्तर 17 दिसंबर, 2025 को दिया जाना है ।

26 अग्रहायण, 1947 (शक)

राष्ट्रीय साइबर सुनम्य निधि

2823. डॉ. जयंत कुमार राय:

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

(क) सीईआरटी-इन के अंतर्गत महत्त्वपूर्ण अवसंरचना संस्थाओं के लिए अनिवार्य सुरक्षा संपरीक्षा की कार्यनीति क्या है;

(ख) सरकार रैनसमवेयर आक्रमणों और सीमा-पार से साइबर अपराध की घटनाओं में वृद्धि से किस प्रकार निपट रही है;

(ग) क्या उद्योग को सशक्त बनाने के प्रयासों में सहायता के लिए एक राष्ट्रीय साइबर सुनम्य निधि स्थापित की गई है;

(घ) सरकार द्वारा पूरे देश में प्रमाणित साइबर सुरक्षा पेशेवरों के प्रतिभा पूल को बढ़ाने के लिए क्या कदम उठाए जा रहे हैं; और

(ङ) साइबर सुरक्षा केंद्रों का प्रभावी क्षेत्रीय साइबर घटना प्रतिक्रिया प्रदान करने के लिए किस प्रकार विस्तार किया जा रहा है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से **(ङ):** भारत सरकार की नीतियों का उद्देश्य एक सुरक्षित, विश्वसनीय और जवाबदेह साइबर स्पेस सुनिश्चित करना है। यह भारत के डिजिटल बुनियादी ढांचे के लिए साइबर खतरे के प्रति सतर्क और पूरी तरह से सचेत है।

इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (सर्ट-इन) और नेशनल क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (एनसीआईआईपीसी) महत्वपूर्ण क्षेत्रों सहित डिजिटल सेवाओं की सुरक्षा के लिए लगातार काम करते हैं।

ये एजेंसियां नियमित रूप से घटनाओं की निगरानी करती हैं, समय पर प्रतिक्रिया का समर्थन करती हैं और बहाली सुनिश्चित करती हैं। वे सूचना प्रौद्योगिकी अधिनियम और उसके अंतर्गत बनाए गए नियमों के अंतर्गत सुरक्षा और सुभेद्यता लेखा परीक्षा करते हैं।

इस संबंध में, सर्ट-इन ने साइबर सुरक्षा ऑडिट करने के लिए जुलाई 2025 में एक व्यापक साइबर सुरक्षा ऑडिट नीति दिशानिर्देश विकसित और जारी किए हैं। ये ऑडिट महत्वपूर्ण बुनियादी ढांचे सहित सभी क्षेत्रों में सुसंगत, प्रभावी और सुरक्षित तरीके से किए जाते हैं। दिशा-निर्देशों के अनुसार, साइबर सुरक्षा ऑडिट वर्ष में कम से कम एक बार किया जाता है। इसने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और ऑडिट करने के लिए 231 सुरक्षा ऑडिटिंग संगठनों को सूचीबद्ध किया है।

इसके अलावा, सरकार ने रैंसमवेयर और सीमा पार साइबर अपराध सहित साइबर इकोसिस्टम की सुरक्षा को मजबूत करने के लिए कई उपाय किए हैं:

1. सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत साइबर सुरक्षा घटनाओं का जवाब देने के लिए सीईआरटी-इन को राष्ट्रीय एजेंसी के रूप में नामित किया गया है।
2. यह नियमित रूप से एआई और जवाबी उपायों का उपयोग करके दुर्भावनापूर्ण हमलों सहित नवीनतम साइबर खतरों/कमजोरियों के बारे में अलर्ट और सलाह जारी करता है।
3. यह प्रभावित संगठनों को उपचारात्मक उपायों की सलाह देता है और घटना प्रतिक्रिया उपायों का समन्वय करता है।

4. राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) सर्ट-इन सूचीबद्ध एजेंसियों के माध्यम से रैंसमवेयर हमलों की बढ़ती संख्या को संबोधित करने के लिए अपने महत्वपूर्ण बुनियादी ढांचे के लिए सालाना व्यापक सुरक्षा ऑडिट करता है, जिसमें शामिल हैं:
   क) केंद्रीय मंत्रालयों/विभागों, राज्यों/केंद्र शासित प्रदेशों और राष्ट्रीय डेटा केंद्रों की सूचना और संचार प्रौद्योगिकी अवसंरचना लेखा परीक्षा।
   ख) महत्वपूर्ण वेब एप्लीकेशन/डेटाबेस/प्लेटफार्मों का व्यापक सुरक्षा ऑडिट।
   ग) एंडपॉइंट प्रोटेक्शन के लिए केंद्रीय मंत्रालयों और विभागों में यूनिफाइड एंडपॉइंट मैनेजमेंट, एंडपॉइंट डिटेक्शन और रिस्पांस सॉल्यूशंस की तैनाती।
   घ) नेटवर्क से अप्रचलित और विरासत प्रणालियों को हटाना.24×7 एआई/एमएल और उन्नत सुरक्षा उपकरणों का उपयोग करके साइबर खतरों की निगरानी, पता लगाना और शमन करना।
   ड़) निरंतर भेद्यता आकलन, सिस्टम सख्त और अनुप्रयोग/सिस्टम कमजोरियों की सक्रिय पहचान।
   च) एनआईसी के आईसीटी बुनियादी ढांचे में जीरो ट्रस्ट सुरक्षा का कार्यान्वयन।
   छ) सरकारी कर्मचारियों के लिए नियमित साइबर सुरक्षा जागरूकता कार्यक्रम।
5. 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।
6. साइबर सुरक्षा की स्थिति और विभिन्न संगठनों की तैयारियों का आकलन करने में सक्षम बनाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित किए जाते हैं।
7. संबंधित क्षेत्रों के भीतर साइबर घटनाओं की निगरानी और प्रतिक्रिया देने के लिए सीएसआईआरटी-फिन (वित्त) और सीएसआईआरटी-पावर जैसे क्षेत्र-विशिष्ट कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीमों (सीएसआईआरटी) की स्थापना।
8. साइबर हमलों का मुकाबला करने और समन्वित वसूली को सक्षम बनाने के लिए सभी सरकारी निकायों के लिए साइबर संकट प्रबंधन योजना (सीसीएमपी) तैयार करना।
9. सभी संगठनों में तैयारियों को मजबूत करने के लिए 213 सीसीएमपी संवेदीकरण कार्यशालाएं आयोजित की गई हैं।
10. विदेशी समाधानों पर निर्भरता कम करने के लिए सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग द्वारा स्वदेशी साइबर सुरक्षा उपकरणों का विकास।

साइबर सुरक्षा प्रतिभा पूल का विस्तार

- इंटरनेट का उपयोग करते समय उपयोगकर्ताओं के बीच जागरूकता पैदा करने के लिए सूचना सुरक्षा शिक्षा और जागरूकता ("आईएसईए") कार्यक्रम शुरू किया गया है।
  - सूचना सुरक्षा जागरूकता के लिए एक समर्पित वेबसाइट बनाई गई है जो नियमित आधार पर प्रासंगिक जागरूकता सामग्री उत्पन्न और उन्नत करती है और इसे https://www.infosecawareness.in पर एक्सेस किया जा सकता है।
- सितंबर 2024 में सर्ट-इन द्वारा शुरू किया गया आर्टिफिशियल इंटेलिजेंस में प्रमाणित सुरक्षा पेशेवर (सीएसपीएआई) कार्यक्रम साइबर सुरक्षा पेशेवरों को एआई सिस्टम को सुरक्षित करने के कौशल से लैस करता है।
  - यह एआई से संबंधित खतरों को संबोधित करने में मदद करता है, और अंततः व्यावसायिक वातावरण में भरोसेमंद एआई तैनाती सुनिश्चित करता है।

साइबर स्वच्छता केंद्र (सीएसके)

यह सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है, 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 सर्वोत्तम अभ्यास भी प्रदान करता है
- उपचारात्मक उपायों के साथ-साथ बॉटनेट/मैलवेयर संक्रमण और कमजोर सेवाओं के बारे में दैनिक आधार पर सभी क्षेत्रों के संगठनों को अलर्ट भेजे जाते हैं।

******