साइबर सुरक्षा

प्रलिमि्स के लयि:

साइबर सुरक्षति भारत पहल, साइबर स्वच्छता केंद्र, ऑनलाइन साइबर अपराध रपिोर्टगि पोर्टल।

मेन्स के लयि:

साइबर सुरक्षा का मुद्दा तथा आवश्यक सुरक्षा उपाय।

चर्चा में क्यों?

हाल ही में **सरट-इन (CERT-In)** ने सभी सरकारी और नजिी एजेंसयिों को साइबर सुरक्षा उल्लंघन की घटनाओं को रपिोर्ट करने के साथ छह घंटे के अंदर अनवािर्य रूप से सूचति करने के लयि कहा है।

- CERT-In को सूचना प्रौद्योगिकी अधनियिम की धारा 70B के तहत साइबर सुरक्षा घटनाओं पर जानकारी एकत्र करने, वशि्लेषण करने और प्रसारति करने का अधकािर है।

CERT-In के बारे में:

- **कंप्यूटर इमरजेंसी रसि्पांस टीम -** इंडयिा भारतीय साइबर स्पेस को सुरक्षति करने के उद्देश्य से इलेक्ट्रॉनकि्स और सूचना प्रौद्योगिकी मंत्रालय का संगठन है।
- यह एक नोडल एजेंसी है जसिका कार्य हैकगि और फशिगि जैसे साइबर सुरक्षा खतरों से नपिटना है।
- यह संगठन साइबर घटनाओं पर जानकारी को एकत्र करने, उसका वशि्लेषण और प्रसार करता है, साथ ही साइबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।
- CERT-In घटना नवािरण और प्रतक्रियिा सेवाओं के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवाएँ भी प्रदान करता है।

CERT-In के नर्दिेश:

- **अनवािर्य रूप से लॉग्स को सक्षम बनाना :**
  - यह सभी सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों, कॉरपोरेट्स और सरकारी संगठनों को अपनी सूचना और संचार प्रौद्योगिकी (Information and Communication Technology- ICT) प्रणाली के लॉग्स को अनवािर्य रूप से सक्षम करने का नर्दिेश देता है।
    - सभी सेवा प्रदाताओं को 180 दनिों की रोलगि अवधकि के लयि लॉग्स को सुरक्षति रूप से बनाए रखना होता है, जसिे भारतीय अधकिार क्षेत्र में रखा जाएगा।
      - यह लॉग कसिी भी **घटना की रपिोर्टगि के साथ या कंप्यूटर आपातकालीन प्रतक्रियिा टीम** के नर्दिेश पर **CERT-In** को प्रदान की जानी चाहयि।
- **सभी ICT प्रणालयिों को जोड़ना और समक्रमकि(Synchronize)करना:**
  - यह सुनशि्चति करने के लयि कि घटनाओं की शृंखला समय-सीमा में सटीक रूप से परलिक्षति हो,**सभी सेवा प्रदाताओं को अपनी सूचना और संचार प्रौद्योगिकी प्रणाली से युक्त क्लॉक को राष्ट्रीय सूचना वज्ञिान केंद्र (NIC) या राष्ट्रीय भौतिक प्रयोगशाला (NPL) के नेटवर्क टाइम प्रोटोकॉल (NTP) सर्वर** से जोड़ने और करने का नर्दिेश दयिा गया है।
    - नेटवर्क टाइम प्रोटोकॉल(NTP) एक ऐसा प्रोटोकॉल है जसिका उपयोग TCP/IP-आधारति नेटवर्क पर वशि्वसनीय रूप से सटीक समय स्रोतों को प्रसारति करने और प्राप्त करने के लयि कयिा जाता है।
    - इसका उपयोग कंप्यूटर की आंतरकि क्लॉक को एक सामान्य समय स्रोत से समक्रमकि करने के लयि कयिा जाता है।
- **रकिॉर्ड बनाए रखने की आवश्यकता:**

    - पाँच साल की अवधि के लिये KYC और वित्तीय लेन-देन का रिकॉर्ड बनाए रखने हेतु इसे वर्चुअल परिसंपत्ति, एक्सचेंज और कस्टोडियन वॉलेट प्रदाताओं की आवश्यकता होती है।
        - क्लाउड, वर्चुअल प्राइवेट नेटवर्क (VPN) प्रदान करने वाली कंपनियों को ग्राहकों के नाम, ईमेल और आईपी पते भी पंजीकृत करने होंगे।

ऐसे पहल की आवश्यकता क्यों :

- **समस्या समाधान की बाधाएँ दूर करना:**
    - यह साइबर सुरक्षा घटनाओं से निपटने तथा विश्लेषण में बाधा संबंधी मुद्दों के मामले में मदद प्रदान करेगा।
- **प्रतिदिन अभिलेखों को सुव्यवस्थित करना:**
    - अतीत में ऐसे मामले सामने आए हैं जहाँ गैर-भंडारण या डेटा की उपलब्धता और मध्यस्थों तथा सेवा प्रदाताओं के साथ उचित रिकॉर्ड के मामलों की पहचान की गई है।
    - ये दिशा-निर्देश बनाये रखने के लिए तारीख के रिकॉर्ड को सुव्यवस्थित करेंगे और CERT-In को सुरक्षा से संबंधित घटनाओं की उचित रिपोर्टिंग करेंगे।
- **उपयोगकर्त्ताओं को उनके अधिकारों के बारे में बताना:**
    - अंतिम उपयोगकर्त्ता को यह जानने का अधिकार है कि क्या उनका डेटा लोड किया गया है ताकि कोई व्यक्ति लेन-देन की धोखाधड़ी, नकली ऋण, आईडी के दुरुपयोग आदि से अपनी रक्षा कर सके।
    - सरकार को भी कंपनियों को घटना के 24 घंटे के भीतर उपयोगकर्त्ताओं को सूचित करने के लिये बाध्य करना चाहिये।
    - कई उपयोगकर्ता अभी भी इस बात से अनभिज्ञ हैं कि उनका केवाईसी (अपने ग्राहक को जानें) और वित्तीय डेटा सुरक्षित है या नहीं।

साइबर सुरक्षा हेतु सरकार की पहलें:

- **साइबर सुरक्षित भारत पहल**
- **साइबर स्वच्छता केंद्र**
- **ऑनलाइन साइबर क्राइम रिपोर्टिंग पोर्टल**
- **भारतीय साइबर अपराध समन्वय केंद्र (I4C)**
- **राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)**
- **सूचना प्रौद्योगिकी अधिनियम, 2000**
- **राष्ट्रीय साइबर सुरक्षा रणनीति 2020**

आगे की राह

- भारत वैश्विक स्तर पर 17 डिजिटल रूप से सशक्तअर्थव्यवस्थाओं में **सबसे तेज़ी से डिजिटल व्यवस्था अपनाने वाले देशों में से एक** है तथा तेज़ी से डिजिटलीकरण के लिये साइबर सुरक्षा को बढ़ावा देने हेतु दूरगामी उपायों को अपनाने की आवश्यकता है।
- कॉरपोरेट्स या संबंधित सरकारी विभागों के लिये यह महत्त्वपूर्ण है कि वे अपने संगठनों में कमियों का पता लगाएँ और उन कमियों को दूर करने के लिये उचित सुरक्षा प्रणाली अपनाएँ, जिसमें विभिन्न स्तरों के बीच सुरक्षा खतरे की खुफिया जानकारी साझा हो सके।
- विभिन्न एजेंसियों और मंत्रालयों के बीच परिचालन हेतु समन्वय सुनिश्चित करने के लिये एक शीर्ष निकाय की आवश्यकता है।

यूपीएससी सिविल सेवा परीक्षा, विगत वर्षों के प्रश्न (PYQs):

प्रश्न. भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (2017)

1. सेवा प्रदाताओं
2. डेटा केंद्र
3. कॉर्पोरेट निकाय

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

- सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act) की धारा 70 B के अनुसार, केंद्र सरकार ने अधिसूचना द्वारा घटना प्रतिक्रिया के लिये राष्ट्रीय एजेंसी के रूप में कार्य करने हेतु भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम **(CERT-In)** नामक एक एजेंसी का गठन किया गया है।

- केंद्र सरकार ने आईटी अधिनियम, 2000 की धारा 70 B के तहत वर्ष 2014 में CERT-In के लिये नियम स्थापित और अधिसूचित किये। नियम 12 (1) (A) के अनुसार, घटना होने के उचित समय के भीतर **CERT-In** को साइबर सुरक्षा की घटनाओं के लिये सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों और कॉर्पोरेट निकायों हेतु रिपोर्ट करना अनिवार्य है। **अतः विकल्प (d) सही है।**

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/cyber-security-18