साइबर सुरक्षा अभ्यास

हाल ही में **कंप्यूटर इमरजेंसी रिस्पांस टीम - इंडिया (CERT-In)** ने **'इंटरनेशनल काउंटर रैनसमवेयर इनिशिएटिव'** के हिस्से के रूप में 13 देशों के साथ **साइबर सुरक्षा अभ्यास "सिनर्जी"** को सफलतापूर्वक डिज़ाइन और संचालित किया।

- यह अभ्यास 'इंटरनेशनल काउंटर रैनसमवेयर इनिशिएटिव- रेजिलिएंशन वर्किंग ग्रुप' के हिस्से के रूप में आयोजित किया गया था, जिसका नेतृत्व राष्ट्रीय सुरक्षा परिषद सचिवालय (NSCS) के नेतृत्व में भारत कर रहा है।

CERT-In:

- **कंप्यूटर इमरजेंसी रिस्पांस टीम - इंडिया (CERT-In)**, भारतीय साइबर क्षेत्र को सुरक्षित करने के उद्देश्य से इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय का संगठन है।
- यह एक नोडल एजेंसी है जिसका कार्य हैकिंग और फ़िशिंग जैसे साइबर सुरक्षा खतरों से निपटना है।
- यह संगठन साइबर घटनाओं पर जानकारी को एकत्र करने, उसका विश्लेषण और प्रसार करता है, साथ ही साइबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।
- CERT-In घटना निवारण और प्रतिक्रिया सेवाओं के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवाएँ भी प्रदान करता है।

सिनर्जी:

- **परिचय:**
  - सिनर्जी एक साइबर सुरक्षा अभ्यास है, जिसे CERT-In द्वारा सिंगापुर की साइबर सुरक्षा एजेंसी (CSA) के सहयोग से सफलतापूर्वक डिज़ाइन और संचालित किया गया है।
  - यह अभ्यास परिदृश्य वास्तविक जीवन की साइबर घटनाओं से लिया गया था, जिसमें घरेलू स्तर की (सीमित प्रभाव वाली) रैनसमवेयर की एक घटना जटिल होकर वैश्विक साइबर सुरक्षा संकट का रूप ले लेती है।
  - प्रत्येक राज्य ने एक राष्ट्रीय संकट प्रबंधन टीम के रूप में भाग लिया, जिसमें राष्ट्रीय सीईआरटी/सीएसआईआरटी, कानून प्रवर्तन एजेंसियों (एलईए), संचार तथा आईटी/आईसीटी मंत्रालय और सुरक्षा एजेंसियों सहित विभिन्न सरकारी एजेंसियों के लोग शामिल थे।
- **उद्देश्य:**
  - **रैनसमवेयर** और जबरन वसूली के उद्देश्य से किये गए साइबर हमलों के खिलाफ सुदृढ़ नेटवर्क बनाने हेतु सदस्य-देशों के बीच विभिन्न रणनीतियों एवं कार्यप्रणालियों का आकलन व आदान - प्रदान करना और उन्हें बेहतर बनाना था।
- **थीम**:
  - "रैनसमवेयर हमलों से निपटने के लिये सुदृढ़ नेटवर्क बनाना"

रैंसमवेयर:

- रैंसमवेयर एक मैलवेयर है जिसे किसी उपयोगकर्ता या संगठन को उनके कंप्यूटर पर फ़ाइलों तक पहुंच से वंचित करने के लिए डिज़ाइन किया गया है।
- इन फाइलों को एन्क्रिप्ट करके और डिक्रिप्शन कुंजी के लिये फिरौती भुगतान की मांग करके, साइबर हमलावर संगठनों को ऐसी स्थिति में रखते हैं जहाँ फिरौती का भुगतान करना उनकी फ़ाइलों तक पहुँच हासिल करने का सबसे आसान और सस्ता तरीका है।
- रैंसमवेयर पीड़ितों को फिरौती का भुगतान करने के लिये मजबूर करने हेतु कुछ वेरिएंट ने अतिरिक्त कार्यक्षमता को जोड़ा है - जैसे क्रेडिट चोरी ।

साइबर सुरक्षा के लिये सरकार की पहल:

- साइबर सुरक्षित भारत पहल
- साइबर स्वच्छता केंद्र
- ऑनलाइन साइबर क्राइम रिपोर्टिंग पोर्टल

- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- राष्ट्रीय महत्तत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)
- सूचना प्रौद्योगिकी अधिनियम, 2000
- राष्ट्रीय साइबर सुरक्षा रणनीति 2020

स्रोत: पी.आई.बी.

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