मुख्य सूचना सुरक्षा अधिकारियों के लिये दिशा-निर्देश

चर्चा में क्यों?

सूचना एवं प्रौद्योगिकी मंत्रालय ने मुख्य सूचना सुरक्षा अधिकारियों के लिये नए दिशा-निर्देश जारी किये हैं। साइबर सुरक्षा संबंधी जोखिमों के विषय में जागरूकता फैलाने के लिये मंत्रालय द्वारा इन नए दिशा-निर्देश में 8 सर्वोत्तम कार्यप्रणालियों को विशेष रूप से स्पष्ट किया गया।

वर्तमान स्थिति

- डिजिटल सुरक्षा फर्म गेमाल्टो की एक रिपोर्ट के मुताबिक, 2017 में भारत में 29 आँकड़ों के उल्लंघन (Data Breach) की घटनाओं में से 28 फीसदी सरकारी महकमे से जुड़ी थीं। इनमें से 21 फीसदी खुदरा, 17 फीसदी शिक्षा और 7 फीसदी स्वास्थ्य सेवा क्षेत्र से संबंधित मामले थे।
- 2017 में घटित लगभग 77% घटनाओं में डाटा उल्लंघन के संबंध में "identity theft" सबसे अहम था। डाटा उल्लंघन के दूसरे सर्वाधिक प्रचलित प्रकार का "सरकारी आँकड़ों तक पहुँच" के रूप में प्रयोग किया गया।

प्रमुख 8 कार्यप्रणालियाँ

सूचना एवं प्रौद्योगिकी मंत्रालय द्वारा जारी दिशा-निर्देशों में मुख्य सूचना सुरक्षा अधिकारियों द्वारा अनुसरण किये जाने के लिये निम्नलिखित 8 प्रमुख कार्यप्रणालियों का उल्लेख किया गया है:

- कंप्यूटर और नेटवर्क उपकरणों की एक विस्तृत जाँच और विभाग द्वारा प्रबंधित सभी प्रकार के आँकड़ों (data) की पहचान करके आईटी परिवेश के विषय में जानकारी प्राप्त करना।
- साइबर हमलों और सुरक्षित साइबर कार्यकलापों जैसे कि मज़बूत पासवर्ड, कई चरणों वाला प्रमाणीकरण, सुरक्षित इंटरनेट ब्राउज़िंग, सोशल मीडिया सुरक्षा, यूएसबी उपकरणों का उपयोग इत्यादि के लिये कर्मचारियों को शिक्षित करना और प्रशिक्षण देना।
- विभाग के लिये सूचना सुरक्षा नीति की समीक्षा करने के साथ-साथ उसमें आवश्यक सुधार करना।
- वास्तविक हार्डवेयर और सॉफ्टवेयर प्राप्त करना तथा ऑपरेटिंग सिस्टम को नियमित रूप से सामयिक बनाना।
- एक औपचारिक साइबर सुरक्षा नीति फ्रेमवर्क लागू करना जिसमें प्रशासन, जोखिम प्रबंधन, अनुपालन, डाटा बैक-अप, प्रवर्तन और उपयोग नीति वक्तव्य शामिल हों।
- गूढ़लेखन (encryption) के साथ मज़बूत डिवाइस सुरक्षा बनाना तथा अभिलेखों (logs) को सुरक्षित बनाए रखने के अलावा आँकड़ों (data) को लीक होने से बचाना।
- साइबर सुरक्षा की व्यापक और नियमित समीक्षा करना।
- साइबर-प्रतिक्रिया की रणनीति के साथ मिलकर सिस्टम प्रक्रियाओं पर निगरानी रखने और अनियमितताओं का पता लगाने के लिये उपकरणों का प्रयोग करना।

गेमाल्टो के अनुसार

- गेमाल्टो के अनुसार, वर्ष 2017 के दौरान भारत में कुल 3.24 मिलियन अभिलेखों (Records) की चोरी हुई या इतने ही अभिलेखों की सुरक्षा में सेंध लगी।
- ऐसी स्थिति में आँकड़ों की गोपनीयता या निजता के उल्लंघन संबंधी घटनाओं पर नियंत्रण रखने के लिये एनक्रिप्शन (गूढ़लेखन), प्रमुख प्रबंधन तथा उपयोगकर्त्ता पहुँच प्रबंधन (User access management) जैसा एक व्यवस्थापन होना चाहिये जो विश्वसनीय होने के साथ-साथ यह सुनिश्चित कर सके कि आँकड़ों की शुद्धता के साथ कोई छेड़छाड़ नहीं की गई है।
- हेराफेरी की चिंताओं के बावजूद, यह व्यवस्था आँकड़ों को सुरक्षित रखने और चोरी हो जाने पर उस डाटा का प्रयोग नहीं किये जाने का आश्वासन देती है।

भारत में लगभग 5.62 लाख लोगों की व्यक्तिगत जानकारी फेसबुक से "चोरी होने" के बाद डाटा संरक्षण और गोपनीयता पर बहस के मुद्दे ने केंद्रीय स्वरूप धारण कर लिया है। स्पष्ट रूप से ऐसी स्थिति में सरकार के साथ-साथ आवाम को भी इस विषय में और अधिक सतर्क होने की आवश्यकता है।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/guidelines-for-chief-information-security-officers