साइबर हमलों की रिपोर्टिंग जरूरी है

हाल ही में इलेक्ट्रानिक्स सूचना प्रौद्योगिकी मंत्रालय ने नए साइबर सुरक्षा नियमों को लाने का संकेत दिया है। इस विनियमन का मुख्य ध्येय, संगठनों पर होने वाले किसी भी साइबर अपराध की रिपोर्ट करने की जिम्मेदारी डालना होगा।

क्या कहता है कानून ?

डेटा संरक्षण विधेयक 2021 के खंड 25 के अनुसार डेटा न्यासियों (फिडयूश्टीज) को किसी भी व्यक्तिगत और गैर-व्यक्तिगत डेटा उल्लंघन की रिपोर्ट करनी चाहिए। उल्लंघन की रिपोर्ट 72 घंटे के अंदर की जानी चाहिए।

यूरोपीय संघ के डेटा मानक को अभी तक गोल्डन स्टैण्डर्ड का माना जाता है। इसमें भी एक निश्चित समय के भीतर डेटा उल्लंघन की घटना की रिपोर्ट करने के लिए एक खंड है।

रिपोर्ट क्यों नहीं की जाती ?

किसी भी संगठन या कंपनी पर डेटा के उल्लंघन की घटना का नकारात्मक प्रभाव पड़ता है। एक अध्ययन से पता चलता है कि ऐसी घटनाओं से लगभग तीन महीने के अंदर ही कंपनी के शेयर 3.5% औसतन गिर जाते हैं। एक वर्ष की अवधि में तो यह प्रभाव दोगुना हो जाता है। इन घटनाओं के चलते ऐसी कंपनियों का बाजार में खराब प्रदर्शन देखा जाता है।

संभावित समाधान -

1. सरकार को चाहिए कि सभी सरकारी विभागों व अन्य संगठनों में समय-समय पर साइबर सुरक्षा प्रभाव आकलन के संचालन के लिए तीसरे पक्ष के साइबर सुरक्षा ऑडिटर्स को सूचीबद्ध करे।

2. निजी फर्मों के लिए समय-समय पर सुरक्षा ऑडिट रिपोर्ट का प्रकाशन अनिवार्य हो। प्रवर्तन के लिए सरप्राइज सुरक्षा ऑडिट करने की व्यवस्था की जाए।

3. आईटी सुरक्षा उत्पादों और सुरक्षा प्रोफाइल का मूल्यांकन और प्रमाणित करने के लिए देशभर में सामान्य मानदंड परीक्षण प्रयोगशालाओं और प्रमाणन निकायों का दायरा साइबर सुरक्षा ऑडिट और आकलन तक बढ़ाया जाए।

4. आईबीएम की तरह, अन्य बड़ी कंपनियों को भी एक बड़ा साइबर सुरक्षा कमांड सेंटर स्थापित करने के लिए प्रोत्साहित किया जा सकता है।

इस तरह के उपायों से भारत उन देशों के समूह के करीब पहुंच जाएगा, जिनके पास समान स्तर की साइबर सुरक्षा और यूरोपियन यूनियन के समान डेटा सुरक्षा है। इससे डेटा का निर्बाध प्रवाह हो सकेगा।

'द हिंदू' में प्रकाशित वी. श्रीधर के लेख पर आधरित। 1 मार्च, 2022