साइबर हमलों को रोकने के लिये नई प्रौद्योगिकियों में निवेश

चर्चा में क्यों?

साइबर खतरों में तेज़ी से बढ़ोतरी के साथ ही सुरक्षा सेवा प्रदाताओं के उत्पादों की मांग में वृद्धि देखी जा रही है, जिसने उन्हें साइबर हमलों को रोकने के लिये नवीनतम तकनीकों और मशीन लर्निंग में निवेश करने को प्रेरित किया है। बैंकिंग क्षेत्र के लिये बी 2 बी साइबर सुरक्षा सेवा प्रदाता, पैलाडियन नेटवर्क के कारोबार में पिछले दो वर्षों के दौरान 30 प्रतिशत की वृद्धि देखी गई है।

सुरक्षा पर खर्च

- बड़े उद्यम अब साइबर सुरक्षा में अपने आईटी व्यय का लगभग 10-15 प्रतिशत निवेश कर रहे हैं। चेन्नई स्थित यूज़र आधारित K7 कंप्यूटिंग प्राइवेट लिमिटेड, एंटी-वायरस सॉफ्टवेयर और इंटरनेट सिक्योरिटी सोल्युशन ने विगत वर्षों में तेज़ी से निवेश को बढ़ाया है।
- उदाहरण के लिये 2010 में कंपनी के 800 सक्रिय उपयोगकर्त्ता थे, लेकिन अब इसमें 5,000 दैनिक उपयोगकर्त्ता हैं। कंपनी अब अपने बी 2 बी सेगमेंट का विस्तार करने पर ध्यान केंद्रित कर रही है।
- हालिया रिपोर्ट के अनुसार, साइबर सुरक्षा बाज़ार के 2018-2023 के बीच 19 प्रतिशत की दर से बढ़ने का अनुमान है। बाज़ार का आकार वृहद् रूप से बढ़ने की संभावना के साथ ही इसके करीब 1,000 करोड़ रुपए होने का अनुमान है।

चुनौतियाँ

- उद्यमियों का कहना है कि इस क्षेत्र में बड़ी चुनौतियाँ भी हैं। विकसित प्रौद्योगिकियाँ नए व्यावसायिक मॉडल को जन्म देती हैं जो खतरे की संभावना को बढ़ाती हैं| ऐसे में ग्राहकों का विश्वास प्राप्त करने के लिये उत्पादों के संबंध में लगातार नवाचार किया जाना आवश्यक है|
- सोफोस, जो कि एंडपॉइंट सुरक्षा सेवा प्रदाता है, द्वारा किये गए 'एंडपॉइंट सिक्योरिटी सर्वे' के मुताबिक भारत में 90% व्यवसायों को या तो नुकसान पहुँचाया गया है या उन्हें रैनसमवेयर (ransomware) द्वारा नुकसान पहुँचाए जाने की आशंका है।
- सर्वेक्षण में पाया गया कि पारंपरिक एंडपॉइंट सिक्योरिटी अब विकसित रैनसमवेयर खतरों के विरुद्ध सुरक्षा प्रदान करने के लिये पर्याप्त नहीं है।

नए समाधान

- कंपनियों, उपक्रमों और सुरक्षा फर्मों ने इसे गंभीरता से लिया है तथा इसके समाधान के लिये निवेश बढ़ाना शुरू कर दिया है।
- कंपनियाँ K7 कंप्यूटिंग इंफ्रास्ट्रक्चर इंटेलिजेंस (AI) और मशीन लर्निंग (ML) जैसे उन्नत तकनीकों का उपयोग करके अधिक मालवेयर को ट्रैप करने हेतु कंप्यूटिंग पावर बढ़ाने को बुनियादी ढाँचे में अधिक निवेश कर रही है।
- इन प्रौद्योगिकियों का उपयोग साइबर हमलों के विभिन्न पैटर्न को समझने के लिये किया जाता है और पहचान को अधिक सटीक और भरोसेमंद बनाने के लिये वैश्विक हमला पैटर्न को भी शामिल किया जाता है।
- यह देखने के लिये भी काम किया जा रहा है कि इन तकनीकों का उपयोग करके हमले को कितनी तेज़ी से पहचाना और रोका जा सकता है| इसमें बदलते प्रौद्योगिकी परिदृश्य को बनाए रखने के लिये समय-समय पर बड़े स्तर पर उन्नयन कार्य भी शामिल किये गए हैं।

मोबाइल खतरा

- मोबाइल फोन समाधानों पर भी अधिक ध्यान केंद्रित किया गया है क्योंकि स्मार्टफोन की पहुँच लगातार बढ़ रही है।
- AI और ML प्रौद्योगिकियों का लाभ उठाने तथा खतरों के समाधान के लिये मोबाइल सुरक्षा समाधानों को अद्यतन करने पर लगातार काम किया जा रहा है।
- कंपनियाँ मोबाइल सुरक्षा उत्पादों पर भी काम कर रही हैं लेकिन उचित मूल्य निर्धारण जैसे मुद्दों से निपटना मुश्किल है। इस मुद्दे के समाधान का प्रयास किया जा रहा है|