साइबर सुरक्षा की समस्या

साभार: फाइनेंसियल एक्सप्रेस
(30 नवंबर, 2017)

ऋषिकेश कामत (एसोसिएट उपाध्यक्ष - उत्पाद प्रबंधन और विपणन),
नेटमैजिक (एनटीटी कम्युनिकेशंस कंपनी)

यह आलेख सामान्य अध्ययन प्रश्न पत्र-III (विज्ञान एवं प्रौद्योगिकी) से संबंधित है।

निवारण-केंद्रित सुरक्षा पहले असरदार हुआ करती थी, लेकिन आज यह बहुत प्रभावी नहीं है।

सुरक्षा प्रौद्योगिकी में प्रगति के बावजूद और कंपनियों द्वारा अपनाई जाने वाली निवारक उपायों की एक विस्तृत श्रृंखला के बावजूद, हमें वानाक्राई, मीराई बॉट और पेट्या जैसे साइबर हमलों का सामना करना पड़ रहा हैं। वर्तमान में डिवाइस-चालित पारिस्थितिकी तंत्र (मोबाइल, पहनने योग्य, चीजों का इंटरनेट), बहुत सारे परस्पर जुड़े सिस्टम, बहुत सारे खुले प्लेटफार्म उपलब्ध हैं और वैश्विक नेटवर्क पर बड़े डेटा का लेनदेन किया जा रहा है, जिससे साइबर हमलों का खतरा काफी बढ़ गया है। वर्तमान में परिष्कृत मैलवेयर निर्माता और साइबर हमलावर हैं, जिनके पास सिस्टम में प्रवेश करने के कई उपाय मौजूद हैं। फिशिंग, बड़े डीडीओएस और रैनसमवेयर हमलों से सिस्टम में प्रवेश करते है। रोकथाम-केंद्रित सुरक्षा कार्यक्रमों ने पहले असरदार जरूर थे, लेकिन आज यह बिलकुल भी प्रभावी नहीं है। फिर भी हमने देखा है कि बहुत संगठनात्मक प्रयास और संसाधन आवंटन सुरक्षा घटनाओं की रोकथाम की ओर बढ़ता है और पता लगाने और प्रतिक्रिया की ओर बहुत कम अग्रसर है। मैलवेयर हमला एक अच्छा उदाहरण है यह पता लगाने का कि पहचान और प्रतिक्रिया कितना महत्वपूर्ण है। हर गुजरते दिन हैकर्स परिष्कार के उच्च स्तर का निर्माण कर रहे हैं। कुछ महीने पहले हैकर्स ने सिस्को, माइक्रोसॉफ्ट और गूगल सहित तकनीकी डोमेन को लक्षित करने के लिए एक उन्नत टोह प्रणाली का इस्तेमाल किया था। इससे पता चलता है कि प्रतिरक्षा की ओर कदम बढ़ाने के बावजूद, प्रौद्योगिकी के अत्याधुनिक उद्यमों में, अंतत: एक मैलवेयर हमले को रोकने में यह विफल रहता है। पर्याप्त प्रतिक्रिया और उपचार तंत्र के बिना, स्थिति को नियंत्रण में लाये जाने से पहले, नेटवर्क क्रैश सहित बहुत अधिक क्षति हुई है।

वर्तमान में भारत में साइबर सुरक्षा के महत्त्व एवं इसके प्रभाव के प्रति जागरूकता की कमी है। स्वयं अधिकांश कंपनियाँ इसे एक रणनीतिक एजेंडा मानने की बजाय अपने सूचना एवं प्रौद्योगिकी विभाग की एक छोटी-सी घटना मानकर नजरअंदाज कर देती हैं। एक सच्चाई यह भी है कि साइबर सुरक्षा की अनेक छोटी घटनाओं की पहचान ही नहीं हो पाती है तो उनकी रिपोर्टिंग कहाँ से होती होगी।

अत: उद्योग-विशेष के अनुसार साइबर सुरक्षा के उपायों को अपनाये जाने की आवश्यकता है, क्योंकि इसके प्रति विशेष रूप से जागरूकता की कमी है तथा यह सूचना एवं प्रौद्योगिकी सुरक्षा से महत्त्वपूर्ण रूप से भिन्न भी है। गार्टनर सुरक्षा और जोखिम प्रबंधन शिखर सम्मेलन 2017 में, विश्लेषक अर्ल पर्किन्स ने अपने सुरक्षा प्रक्रिया को प्रतिक्रिया और उपचार के लिए स्थानांतरित करने के बारे में बताया। उन्होंने तर्क यह दिया कि जो लोग आपके आईटी सिस्टम में प्रवेश करना चाहते हैं, वे आखिरकार वो अपने मकसद में सफल हो ही जाएंगे, भले ही हमले को रोकने में आपने कितना भी निवेश किया हो। आपके आईटी सुरक्षा कार्यक्रमों की सफलता हमले को रोकने की कोशिश करने पर निर्भर नहीं करती है, बल्कि समय पर हमलों का अनुमान लगाने, पता लगाने और जवाब देने की क्षमता में निर्भर करती है। इसलिए, मजबूत और लम्बे द्वार के निर्माण पर ध्यान देने की बजाय, हमे सुरक्षा घटना की पहचान करने और इसकी प्रतिक्रिया पर ध्यान देने चाहिए। डेटा और एनालिटिक्स एक पूर्वानुमानित और उत्तरदायी खतरे की कमी और घटना प्रबंधन सेट अप के महत्वपूर्ण घटक हैं। अत्यधिक संवेदनशील सुरक्षा प्रबंधन वातावरण बनाने की चुनौतियों में से एक समस्या नेटवर्क और सिस्टम जानकारी एकत्रित और विश्लेषण करना है। प्रक्रिया केवल तभी काम करती है, जब वास्तविक समय डेटा उपलब्ध हो; समय पर निर्णय लेने के लिए सुरक्षा टीमों के पास सही टूल और विशेषज्ञता प्राप्त हो; संगठन के पास उत्तरदायी तंत्र मौजूद हो, जिसमें जोखिम को कम करने के लिए मानकीकृत और परीक्षणित नीतियां शामिल होनी चाहिए तथा सुरक्षाकर्मियों को हमले के दौरान और बाद में क्या किया जाना चाहिए, इसकी जानकारी हो।

निश्चित तौर पर, भारतीय कंपनियों को अपने साइबर सुरक्षा तंत्र को और मजबूत करना होगा। इसकी शुरुआत शीर्ष पर बैठे अधिकारियों को एक विजन बना कर करना चाहिए। कंपनियों के मुख्य कार्यकारी अधिकारियों को अपने प्रबंधन एजेंडे में इसे उच्च प्राथमिकता देनी होगी तथा एक सुपरिभाषित रोड-मैप बनाना होगा।

कंपनियों को अपने महत्त्वपूर्ण परिसंपत्तियों, जिनकी जोखिम की संभावना सर्वाधिक हो, की पहचान कर लेनी चाहिये। इसके अलावा उनको समय-समय पर रियल-टाइम हमलों के मुताबिक नियमित अभ्यास करना चाहिये। इससे उन्हें अपनी तैयारियों को जानने-परखने तथा जवाबी कार्यवाही करने का मौका मिलेगा। सुरक्षा प्रबंधन के लिए एक उत्तरदायी दृष्टिकोण को अपनाने के लिए सीआईओ को गार्टनर द्वारा प्रबंधित डिटेक्शन और रिस्पांस सर्विसेज (एमडीआरएस) के रूप में संदर्भित नए, प्रबंधित सुरक्षा उपायों पर विचार करना होगा, जो शक्तिशाली विश्लेषिकी, कुशल पेशेवर, 24×7 पहचान और प्रतिक्रिया करता है। साइबर हमले से पूरी सुरक्षा का दावा नहीं किया जा सकता, लेकिन बेहतर आपदा प्रबंधन और सुधार की व्यवस्था लागू की जानी चाहिए, ताकि ऐसे हालात में जल्दी से जल्दी व्यवस्था सुधारी जा सके। सीईआरटी- इन तथा अन्य एजेंसियों को ऐसे सिस्टम बनाने चाहिए जो जनता को इनका असर कम करने के उपाय जल्द से जल्द बताएं।

वर्तमान में एक प्रबंधित सुरक्षा सेवा प्रदाता का उपयोग करने वाले संगठन एमडीआरएस को स्थानांतरित करने के लिए एक बेहतर स्थिति में होंगे, क्योंकि उनके पास पहले से ही कुछ मानक प्रतिक्रिया और उपाय तंत्र होंगे। इसके अलावा, सुरक्षा ढांचे के साथ शुरू करने वाली कंपनियों के लिए, सर्वश्रेष्ठ-इन-क्लास प्रबंधित सुरक्षा सेवा प्रदाता का लाभ उठाने और शुरुआत में भी मजबूत पहचान और प्रतिक्रिया क्षमताओं का निर्माण करने का एक शानदार अवसर है।

संबंधित तथ्य

रैनसमवेयर क्या है?

- यह एक प्रकार का मॉलवेयर है जो कंप्यूटर सिस्टम के एक्सेस को ब्लॉक कर देता है और डेटा को चुरा लेता है। इसके बाद साइबर अपराधी आपके डेटा को वापस लौटाने के लिए फिरौती की मांग करते हैं। 'वाना क्राई' रैनसमवेयर विंडो पर आधारित ऑपरेटिंग सिस्टम पर हमला करता है। इसमें डेटा को इनक्रिप्ट कर दिया जाता है और डिस्क्रिप्ट करने के लिए बिटकॉइन की मांग की जाती है।

भारत के लिये चिंता के कारण

- इस प्रकार के हमलों से संग्रहित फिरौती का उपयोग आतंकवाद के वित्तपोषण में किया जा सकता है।
- ऐसे हमले भारतीय सुरक्षा एजेंसियों एवं रक्षा संस्थानों के कंप्यूटरों को प्रभावित कर उनके महत्त्वपूर्ण दस्तावेजों को एनक्रिप्ट कर सकते हैं। जिससे भारत की सुरक्षा व्यवस्था पर गंभीर प्रभाव पड़ सकता है।
- विमुद्रीकरण के पश्चात भारत में डिजिटल लेन-देन को बढ़ावा देने के प्रयास किये जा रहे हैं, लेकिन ऐसे हमले न केवल इन प्रयासों को विफल कर सकते हैं बल्कि डिजिटल इंडिया पहल को भी प्रभावित कर सकते हैं।

क्या है पेट्या रैनसमवेयर?

- पेट्या/नॉटपेट्या (Petya/Notpetya) रैनसमवेयर, एक दुर्भावनापूर्ण सॉफ्टवेयर है, जो कंप्यूटर में फाइलों को लॉक कर देता है और उन फाइलों को अनलॉक करने के लिये उपयोगकर्त्ता से फिरौती की मांग करता है।
- वर्तमान साइबर हमला पेट्या रैनसमवेयर का एक रूपांतर माना जा रहा है, जो वर्ष 2016 से अस्तित्व में है।
- कैस्परस्काई, जो कि एक साइबर सुरक्षा प्रदाता है, के प्रारंभिक जाँच के अनुसार, वर्तमान साइबर हमला पेट्या रैनसमवेयर का एक रूपांतर नहीं है, बल्कि एक नया रैनसमवेयर है। वह इसे नॉटपेट्या कह रही है।
- पेट्या अथवा नॉटपेट्या रैनसमवेयर, वान्नाक्राई (WannaCry) वायरस के बाद दूसरा प्रमुख वैश्विक रैनसमवेयर है, जिसका प्रभाव इतना व्यापक है। गौरतलब हो कि वान्नाक्राई वायरस ने इस वर्ष मई महीने में विश्व के 200 देशों के 3,00,000 कंप्यूटरों को प्रभावित किया था।
- वान्नाक्राई रैनसमवेयर की तरह पेट्या भी अपने आप को प्रचारित करने के साधन के रूप में बाह्य ब्लू (एक्सटर्नल ब्लू) का उपयोग करता है।
- पेट्या रैनसमवेयर न केवल फाइलों को एनक्रिप्ट कर देता है, बल्कि यह सम्पूर्ण डिस्क को लॉक कर देता है, जिससे यह तब तक कार्य करना बंद कर देता है, जब तक इसे हटाया नहीं जाता। यह पूरी कार्य प्रणाली को बंद कर देता है एवं उसे चालू करने के लिये बिटक्वाइनों के रूप में 300 डॉलर फिरौती की माँग करता है।

डिजिटल रूप से सुरक्षित भारत के निर्माण के लिये आवश्यक कदम-

- अधिक कठोर साइबर नीति एवं विनियामक फ्रेमवर्क की स्थापना।
- भारत सरकार को डेटा की सुरक्षा के लिये सर्वोत्तम अंतर्राष्ट्रीय तकनीकी एवं व्यवहार की मदद लेनी चाहिये।
- केंद्र सरकार के द्वारा डिजिटल साक्षरता के साथ-साथ जागरूकता अभियान भी संचालित किये जाने चाहिये।
- साइबर एवं डिजिटल अपराधों के मामले में समुचित एवं कठोर सजा के लिये उपयुक्त प्राधिकरण की स्थापना की जानी चाहिये।
- साइबर सुरक्षा से सबंधित देश की सबसे प्रमुख एजेंसी CERT-IN को और अधिक मजबूत बनाया जाना चाहिये।
- सोशल मीडिया को विनियमित करने के लिये उपयुक्त व्यवस्था की जानी चाहिये क्योंकि सर्वोच्च न्यायालय द्वारा आईटी एक्ट की धारा 66। को रद्द किये जाने के बाद से कोई अन्य व्यवस्था मौजूद नहीं है।

साइबर अपराध क्या है?

- साइबर अपराध वे गैरकानूनी कार्य हैं जिनमें कंप्यूटर का इस्तेमाल होता है तथा सूचना, तकनीकी एवं आपराधिक गतिविधियाँ इसमें शामिल होती हैं। ये अपराध सामान्यत: किसी प्रकार की हिंसा नहीं फैलाते, लेकिन लालच, सम्मान और किसी व्यक्ति के चरित्र के कमजोर पहलू को पकड़कर विभिन्न अपराधों को जन्म देते हैं। साइबर अपराधों में आपराधिक गतिविधियाँ, जैसे-चोरी, धोखा, गबन, अपमान करना आदि सम्मिलित हैं। इनमें व्यक्तिगत, संस्थागत, सामाजिक अपराधों के अलावा हैकिंग, सुरक्षा संबंधी, इंटरनेट पर धोखाधड़ी, पोर्नोग्राफी तथा राष्ट्रीय सुरक्षा जैसे खतरे शामिल होते हैं। सरल शब्दों में कहें तो साइबर अपराध गैरकानूनी कृत्यन है जिसमें कंप्यूटर या तो एक उपकरण या लक्ष्य या दोनों होता है। हमारे देश में साइबर अपराधों में सूचना तकनीक कानून और भारतीय दंड संहिता के तहत आने वाले विभिन्न प्रकार के अपराध शामिल हैं।

संभावित प्रश्न

साइबर हमले से पूरी सुरक्षा का दावा नहीं किया जा सकता, लेकिन बेहतर प्रबंधन और सुधार की व्यवस्था के द्वारा जल्दी से जल्दी व्यवस्था में सुधार लाई जा सकती है। इस कथन के सन्दर्भ में साइबर हमले से बचाव के उपायों का वर्णन करे।

(200 शब्द)

Cyber attack can not be claimed to be full security, but better system can be improved by disaster management and improvement system as soon as possible. Describe the measures to prevent cyber attack in relation to this statement. ***(200 words)***