आधुनिक समय की साइबर सुरक्षा चुनौतियाँ

आधुनिक साइबर सुरक्षा चुनौतियों की जानकारी रखकर स्वयं को सुरक्षित रखें

संपादित : **मोहन दास विस्वम्**

परिष्कृत साइबर खतरों, बढ़े हुए नियमन और तेज़ी से विकसित हो रही तकनीक के कारण साइबर सुरक्षा का परिदृश्य लगातार जटिल होता जा रहा है। संगठनों को अपने उपयोगकर्ताओं की संवेदनशील जानकारी की रक्षा करने के साथ-साथ सहज और आसान उपयोगकर्ता अनुभव प्रदान करना जारी रखने की चुनौती का सामना करना पड़ेगा। यहाँ उन उभरती चुनौतियों और खतरों पर करीब से नज़र डाली गई है जो इस वर्ष सुरक्षा परिदृश्य को आकार देने के लिए तैयार हैं :

एआई-संचालित सामाजिक इंजीनियरिंग खतरे

एआई (आर्टिफिशियल इंटेलिजेंस) की उन्नति के साथ, नेचुरल लैंग्वेज प्रोसेसिंग (एनएलपी) और मशीन लर्निंग (एमएल) पर आधारित एल्गोरिदम का उपयोग करके अत्यधिक विश्वसनीय फ़िशिंग अभियान बनाए जा रहे हैं और डीपफेक तैयार किए जा रहे हैं, जो साइबर हमलों को स्वचालित कर रहे हैं। एआई, सोशल मीडिया प्रोफाइल, ऑनलाइन इंटरैक्शन और लीक हुए डेटा का विश्लेषण करके ऐसे संदेश उत्पन्न कर सकता है जो अधिक प्रामाणिक, लक्षित और विश्वसनीय लगते हैं। हमलावर कंपनी के अधिकारियों का प्रतिरूपण करने वाले विश्वसनीय ऑडियो और वीडियो डीपफेक आसानी से बना सकते हैं ताकि कर्मचारियों को धन हस्तांतरित करने या संवेदनशील गोपनीय जानकारी का खुलासा करने के लिए धोखा दिया जा सके। एआई, कई और अद्वितीय लक्षित संदेशों, प्रतिक्रियाओं या परिदृश्यों को उत्पन्न करके बड़े पैमाने पर सोशल इंजीनियरिंग अभियानों को स्वचालित कर सकता है, जिससे मैनुअल प्रयास की आवश्यकता कम हो जाती है और हमलों की मात्रा बढ़ जाती है।

डिजिटल बुनियादी ढांचे में गलत कॉन्फ़िगरेशन

क्लाउड वातावरण में गलत कॉन्फ़िगरेशन, जैसे कि पहुँच नियंत्रण

आर. बिंदू माधवी
वैज्ञानिक - डी
r.bindumadhavi@nic.in

ए. रमादेवी
वैज्ञानिक - डी
rama.a@nic.in

साइबर खतरे तेज़ी से विकसित हो रहे हैं क्योंकि हमलावर अधिक परिष्कृत होते जा रहे हैं और दुनिया भर में जुड़े हुए उपकरणों की संख्या लगातार बढ़ रही है। रिमोट वर्क और क्लाउड को अपनाने में वृद्धि के साथ, अंतिम बिंदु और डेटा प्रवाह आकर्षक हमले के लक्ष्य बन जाते हैं। इस लेख में, हमने वैश्विक संगठनों को प्रभावित करने वाले नवीनतम साइबर सुरक्षा रुझानों का पता लगाया है, और सूचित रहना आपके जोखिम को कम कर सकता है।

का न होना, असुरक्षित भंडारण स्थान और सुरक्षा नीतियों का अप्रभावी कार्यान्वयन, डेटा उल्लंघनों के सबसे सामान्य कारण हैं। गलत कॉन्फ़िगरेशन हमलावरों को अपनी पहचान छिपाकर क्रिप्टो करेंसी माइनिंग जैसी दुर्भावनापूर्ण गतिविधियों के लिए क्लाउड संसाधनों का अपहरण करने और समझौता किए गए क्लाउड खातों से साइबर हमले शुरू करने में सक्षम बनाता है। कमजोर या अत्यधिक अनुमेय पहुँच प्रबंधन नीतियां उपयोगकर्ताओं या तीसरे पक्ष को उचित सत्यापन के बिना महत्वपूर्ण क्लाउड संसाधनों तक पहुँचने की अनुमति दे सकती हैं, जिससे हमलावरों को इन विशेषाधिकारों का शोषण करने का रास्ता मिल जाता है। क्लाउड सेवाएँ ऐसे एप्लिकेशन प्रोग्रामिंग इंटरफेस (एपीआई) को उजागर कर सकती हैं जो सुरक्षित नहीं हैं या जिन्हें अत्यधिक अनुमतियाँ दी गई हैं, जिससे हमलावरों के लिए उनका फायदा उठाना और क्लाउड संसाधनों तक अनधिकृत पहुँच प्राप्त करना आसान हो जाता है।

मोबाइल उपकरण शोषण

मोबाइल उपकरणों पर बढ़ती निर्भरता के साथ, आने वाले दिनों में इन प्लेटफार्मों पर हमलों में पर्याप्त वृद्धि होने की उम्मीद है। इसमें मोबाइल ऑपरेटिंग सिस्टम, मोबाइल ऐप और 5G जैसी मोबाइल-केंद्रित तकनीकों में कमजोरियों का फायदा उठाना शामिल है। मोबाइल मैलवेयर में महत्वपूर्ण वृद्धि देखी गई है, और यह प्रवृत्ति जारी रहने की उम्मीद है क्योंकि मोबाइल उपकरणों का उपयोग बैंकिंग, खरीदारी और संवेदनशील जानकारी तक पहुँचने के लिए तेजी से किया जा रहा है। समझौता की गई कुंजी के साथ, हमलावर एक मैन-इन-द-मिडिल अटैक में एक सुरक्षित एच.टी.टी.पी.एस. कनेक्शन को एक गैर-एन्क्रिप्टेड एचटीटीपी कनेक्शन में डाउनग्रेड कर सकते हैं, जिससे वे नेटवर्क पर प्रसारित होते समय संवेदनशील जानकारी (जैसे पासवर्ड और क्रेडिट कार्ड नंबर) चुरा सकते हैं। जेलब्रोकन (आईओएस) या रूटेड (एंड्रॉयड) मोबाइल उपकरण हमलावरों को अनधिकृत ऐप या सॉफ़्टवेयर स्थापित करने में सक्षम बनाते हैं और इस प्रकार उपकरण को विभिन्न हमलों के लिए खोल देते हैं।

आईओटी उपकरण की कमजोरियाँ

आईओटी उपकरण (इंटरनेट ऑफ थिंग्स उपकरण) में अक्सर मज़बूत सुरक्षा की कमी पाई जाती है, जिससे वे हमलावरों के लिए आसान लक्ष्य बन जाते हैं जो बॉटनेट्स या अन्य दुर्भावनापूर्ण उद्देश्यों के लिए उपकरणों का अपहरण करना चाहते हैं। स्मार्ट कैमरे और पहनने योग्य उपकरण जैसे आईओटी उपकरण व्यक्तिगत डेटा एकत्र करते हैं। यदि इन पर समझौता होता है, तो ये उपकरण संवेदनशील जानकारी को उजागर कर सकते हैं या निगरानी के लिए उपयोग किए जा सकते हैं। आईओटी उपकरण अक्सर कमजोर एन्क्रिप्शन या असुरक्षित संचार प्रोटोकॉल पर निर्भर करते हैं, जिससे वे अवरोधन और शोषण के शिकार हो जाते हैं। समझौता किए गए आईओटी उपकरणों का उपयोग अक्सर डीडॉस हमलों जैसे बड़े पैमाने पर बॉटनेट हमलों में किया जाता है जो नेटवर्क और सर्वर को अभिभूत कर देते हैं। हमलावर उपयोगकर्ता की जानकारी के बिना क्रिप्टोकरेंसी माइनिंग के लिए अपनी प्रोसेसिंग पावर का उपयोग करने हेतु आईओटी उपकरणों का अपहरण कर सकते हैं। स्मार्ट रेफ्रिजरेटर, कैमरे और यहाँ तक कि गणना शक्ति वाले चिकित्सा उपकरण का भी क्रिप्टो माइनिंग के लिए शोषण किया जा सकता है, जिससे सिस्टम धीमा हो सकता है, हार्डवेयर को नुकसान हो सकता है और बिजली की खपत बढ़ सकती है।

अंदरूनी खतरे

जैसे-जैसे व्यवसाय तेज़ी से डिजिटल और अंतर्संबंधित होते जा रहे हैं, अंदरूनी लोगों - संगठन के भीतर के वे व्यक्ति जिनकी सिस्टम और डेटा तक पहुँच है - से उत्पन्न ख़तरा एक गंभीर चिंता का विषय बना हुआ है। कर्मचारी अनजाने में गलत प्राप्तकर्ताओं को ईमेल भेजकर, क्लाउड सेटिंग्स को गलत तरीके से कॉन्फ़िगर करके, या सुरक्षित संचार विधियों का उपयोग न करके संवेदनशील जानकारी उजागर कर सकते हैं। असंतुष्ट कर्मचारी जानबूझकर कंपनी के

सिस्टम में तोड़फोड़ कर सकते हैं, डेटा चुरा सकते हैं, या संचालन में बाधा डाल सकते हैं यदि उन्हें लगता है कि उनके साथ दुर्व्यवहार हो रहा है या वे अपने नियोक्ता से असंतुष्ट हैं। ठेकेदार और विक्रेता, जो स्थायी कर्मचारियों के समान सुरक्षा प्रोटोकॉल के अधीन नहीं हैं, एक कमज़ोर कड़ी हो सकते हैं। दूर से काम करने वाले या व्यक्तिगत उपकरणों (बीवायओडी) का उपयोग करने वाले कर्मचारी अनजाने में कंपनी नेटवर्क को दुर्भावनापूर्ण सॉफ़्टवेयर या हमलावरों के सामने उजागर कर सकते हैं यदि उनके उपकरण और पहुँच ठीक से सुरक्षित नहीं हैं। दूरस्थ कर्मचारी असुरक्षित नेटवर्क से सिस्टम तक पहुँच सकते हैं, जिससे अनधिकृत व्यक्तियों के लिए डेटा को इंटरसेप्ट करना या कॉर्पोरेट संसाधनों तक पहुँच प्राप्त करना आसान हो जाता है।

एन्क्रिप्शन-रहित रैंसमवेयर हमले

एन्क्रिप्शन-रहित रैंसमवेयर हमले एक नए और विकसित हो रहे खतरे का प्रतिनिधित्व करते हैं जहाँ हमलावर फ़ाइलों को एन्क्रिप्ट करने की पारंपरिक विधि पर निर्भर किए बिना पीड़ितों से फिरौती वसूलते हैं। डेटा को लॉक करने और डिक्रिप्शन कुंजी के लिए फिरौती की माँग करने के बजाय, इन हमलों में आमतौर पर संवेदनशील जानकारी की चोरी या सिस्टम को इस तरह से बाधित करना शामिल होता है जिससे कम तत्काल परिचालन व्यवधान होता है। इस प्रकार हमलावर लंबे समय तक पता चले बिना काम करते हैं, संवेदनशील जानकारी जुटाते हैं और फिर फिरौती का भुगतान न करने पर उसे प्रकाशित करने की धमकी देते हैं। भले ही डेटा एन्क्रिप्टेड न हो, परिणाम फिर भी गंभीर हो सकते हैं, क्योंकि वे महत्वपूर्ण व्यावसायिक संपत्तियों को लक्षित करते हैं और गोपनीयता से समझौता करते हैं। हमलावर रिमोट एक्सेस ट्रोजन या फ़ाइल-रहित मैलवेयर जैसे टूल तैनात करके डेटा एक्सफ़िल्ट्रेशन के अपने तरीकों में अधिक परिष्कृत होते जा रहे हैं, ताकि पारंपरिक पहचान प्रणालियों को ट्रिगर किए बिना डेटा चुराया जा सके। 'रैंसमवेयर-एज-ए-सर्विस' मॉडल, जो कम कुशल हमलावरों को भी विनाशकारी रैंसमवेयर अभियान शुरू करने में सक्षम बनाता है, एक और सुरक्षा चुनौती है जो आधुनिक समय में बढ़ रही है।

डीएनएस टनलिंग खतरे

डोमेन नाम प्रणाली (डीएनएस) ट्रैफ़िक को अक्सर नेटवर्क संचार के सुचारू रूप से कार्य करने को सुनिश्चित करने के लिए नेटवर्क परिधि के पार स्वतंत्र रूप से यात्रा करने का विशेषाधिकार प्राप्त होता है। हमलावर अपने दुर्भावनापूर्ण लक्ष्यों को प्राप्त करने के लिए डीएनएस ट्रैफ़िक का शोषण करने के लिए इस विशेषाधिकार का पता लगाते हैं। डीएनएस टनलिंग एक ऐसी साइबर हमले की तकनीक है जहाँ दुर्भावनापूर्ण अभिनेता डेटा एक्सफ़िल्ट्रेशन या कमांड और नियंत्रण के लिए एक गुप्त संचार चैनल बनाने हेतु डीएनएस प्रोटोकॉल का दुरुपयोग करते हैं। डीएनएस को उसके इच्छित उद्देश्य के लिए उपयोग करने के बजाय, हमलावर डीएनएस प्रश्नों और प्रतिक्रियाओं के भीतर डेटा या कमांड एम्बेड करते हैं। यह उन्हें नेटवर्क सुरक्षा उपायों को बाईपास करने और बिना लाल झंडे उठाए समझौता किए गए सिस्टम के साथ संवाद करने की अनुमति देता है। डीएनएस टनलिंग का पता पेलोड का निरीक्षण करके, असामान्य पैटर्न के लिए डीएनएस प्रश्नों की निगरानी करके और डेटा एन्कोडिंग के संकेतों की पहचान करने के लिए डीप पैकेट निरीक्षण करके लगाया जा सकता है। अन्य निवारक उपायों में नियमित रूप से डीएनएस ट्रैफ़िक की निगरानी करना, डीएनएस सुरक्षा एक्सटेंशन लागू करना, अनधिकृत सर्वर पर डीएनएस ट्रैफ़िक को ब्लॉक करने के लिए फ़ायरवॉल नियम लागू करना और अनावश्यक डीएनएस प्रश्नों को सीमित करना शामिल है।

▲ चित्र 12.1 विकसित होते साइबर खतरे

क्वांटम-संचालित खतरे

जैसे-जैसे दुनिया क्वांटम कंप्यूटिंग के युग की ओर बढ़ रही है, सुरक्षा परिदृश्य में एक महत्वपूर्ण बदलाव आ रहा है। क्वांटम कंप्यूटिंग तकनीक के आगमन में मौजूदा क्रिप्टोग्राफ़िक सिस्टम को बाधित करने और वर्तमान सुरक्षा उपायों को अप्रचलित करने की क्षमता है। क्वांटम-संचालित खतरों की तैयारी आवश्यक हो जाएगी क्योंकि क्वांटम कंप्यूटर विकसित होते हैं और उनकी क्षमताएँ साकार होती हैं, खासकर साइबर सुरक्षा समुदाय के लिए। क्वांटम कंप्यूटर में व्यापक रूप से उपयोग किए जाने वाले सार्वजनिक-कुंजी क्रिप्टोग्राफी एल्गोरिदम को तोड़ने के साथ-साथ सममित-कुंजी क्रिप्टोग्राफी को बाधित करने की क्षमता है। आधुनिक एल्गोरिदम क्वांटम कंप्यूटरों को क्लासिक कंप्यूटरों की तुलना में अनसुलझे डेटाबेस (या ब्रूट-फ़ोर्स एन्क्रिप्शन कुंजियाँ) को तेजी से खोजने की अनुमति देते हैं। यह कुंजी की लंबाई को प्रभावी ढंग से आधा करके एन्क्रिप्शन की सुरक्षा को कम कर देगा, जिससे 128-बिट कुंजियों का उपयोग करने वाले सिस्टम आज के 64-बिट कुंजियों के जितने ही असुरक्षित हो जाएँगे।

ओपन-सोर्स कोड की कमजोरियाँ

ओपन-सोर्स कोड आधुनिक सॉफ़्टवेयर विकास का एक मूलभूत आधार बन गया है, जो डेवलपर्स को मौजूदा टूल्स, फ्रेमवर्क और लाइब्रेरीज़ का लाभ उठाकर अपनी परियोजनाओं को तेज़ी से पूरा करने में सक्षम बनाता है। यह विकास के समय को कम करने, सहयोग बढ़ाने और नवाचार को बढ़ावा देने जैसे कई लाभ प्रदान करता है। हालाँकि, ओपन-सोर्स सॉफ़्टवेयर ये लाभ तो प्रदान करता है, लेकिन साथ ही यह संभावित जोखिम भी लाता है जिनसे संगठनों और डेवलपर्स को अवगत होना चाहिए। दुर्भावनापूर्ण योगदानकर्ता या हमलावर ओपन-सोर्स परियोजनाओं में बैकडोर स्थापित कर सकते हैं, जिनका बाद में सिस्टम तक अनधिकृत पहुँच प्राप्त करने या संवेदनशील डेटा चुराने के लिए उपयोग किया जा सकता है। ये बैक डोरकोड के प्रतीत होने वाले सौम्य भागों में छिपे हो सकते हैं, जिससे उनका पता लगाना मुश्किल हो जाता है। ओपन-सोर्स परियोजनाएँ अक्सर स्वयंसेवकों या छोटी टीमों द्वारा विकसित और अनुरक्षित की जाती हैं, जिनमें व्यापक सुरक्षा परीक्षण का अभाव हो सकता है। अनजाने में लाइसेंस उल्लंघन, लाइसेंस विवाद, विक्रेता समर्थन का अभाव, भेद्यता प्रकटीकरण में जवाबदेही का अभाव, परित्यक्त परियोजनाएँ, खराब दस्तावेज़ीकरण आदि इस मुद्दे को और भी जटिल बना देते हैं।

जनरेटिव एआई मॉडल को खतरे

जैसे-जैसे संगठन अपने संचालन में जनरेटिव एआई को एकीकृत करते हैं, वे अपने हमले की सतह का विस्तार करते हैं। जेनएआई मॉडल डेटा को संसाधित और उत्पन्न करते हैं जिसमें अनजाने में संवेदनशील जानकारी हो सकती है। इन मॉडलों के प्रशिक्षण में उपयोग किए गए गलत, पक्षपातपूर्ण या समझौता किए गए डेटा से डेटा लीक या गोपनीयता का उल्लंघन हो सकता है। जेनएआई सिस्टम विरोधी हमलों से प्रतिरक्षा नहीं हैं, जहाँ हमलावर इनपुट डेटा को इस तरह से हेरफेर करते हैं कि एआई मॉडल अप्रत्याशित रूप से व्यवहार करने लगे या दुर्भावनापूर्ण आउटपुट उत्पन्न करे। हमलावर स्वामित्व वाले जेनएआई मॉडल को रिवर्स-इंजीनियर करने या चोरी करने का प्रयास कर सकते हैं, जिससे बौद्धिक संपदा और अंतर्दृष्टि तक पहुँच प्राप्त होती है जिसका दुर्भावनापूर्ण उद्देश्यों के लिए शोषण किया जा सकता है। इससे बौद्धिक संपदा की चोरी या व्यापार रहस्यों का अवैध उपयोग हो सकता है।

निष्कर्ष

भविष्य की अवधि के लिए ये भविष्यवाणियाँ सक्रिय रक्षा रणनीतियों पर अधिक ध्यान केंद्रित करने की माँग करेंगी। संगठनों को संबंधित नियमों का पालन करके अपनी मूलभूत साइबर सुरक्षा स्थिति में सुधार करने पर ध्यान केंद्रित करना चाहिए। उन्हें ज़ीरो-ट्रस्ट आर्किटेक्चर को प्राथमिकता देनी चाहिए, एआई-संचालित सुरक्षा नियंत्रणों की शक्ति का उपयोग करना चाहिए, और इन खतरों को दूर करने के लिए हितधारकों के बीच सुरक्षा जागरूकता की संस्कृति को बढ़ावा देना चाहिए।

अधिक जानकारी के लिए संपर्क करें

राज्य सूचना अधिकारी
राष्ट्रीय सूचना विज्ञान केंद्र, तमिलनाडु राज्य केंद्र
ई2-ए, राजाजी भवन, बेसेंट नगर
चेन्नई, तमिलनाडु – 600090
ईमेल: sio.tn@nic.in , फ़ोन: 044-44992425