E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

भारत की साइबर सुरक्षा व रणनीति

डॉ. कुलदीप सिंह

राजनीति विज्ञान

Paper Rcevied date

05/05/2025

Paper date Publishing Date

10/05/2025

DOI

https://doi.org/10.5281/zenodo.15453396

IMPACT FACTOR

5.924

ABSTRACT

इन्टरनेट के युग में संगठन साइबर हमलों से खुद को सुरक्षित रखने के लिये आईटी इनहास्ट्रक्चर पर बहुत अधिक निर्भर हैं। जैसे-जैसे अधिक से अधिक संगठन डिजिटल परिवर्तन को अपना रहे हैं, साइबर अपराध का जोखिम तेजी से बढ़ रहा है इसलिए साइवर सुरक्षा का महत्व नी वह रहा है। साइबर सुरक्षा एक ऐसा कवच बन गई है जो हमेशा चमकता रहता है। मजबूत साइबर सुरक्षा नीति और बुनियादी ढाँचा मिलकर कंप्यूटर सिस्टम और नेटवर्क को अनधिकृत इमले या पहुँच से सुरक्षित रखता है। व्यवसाय, व्यक्ति और सरकारें टैकर्स के खिलाफ अपनी संपत्तियों और डेटा की सुरक्षा में साइबर सुरक्षा के लाभों को प्राप्त करने के लिए भारी निवेश कर रही हैं। आज की प्रतिस्पर्धी दुनिया में किसी भी व्यवसाय को जीवित रहने के लिए, उसे सही उपकरण और साइवर सुरक्षा रणनीति की आवश्यकता होती है।

साइबर सुरक्षा व उसका उद्देश्य

साइबर सुरक्षा, सूचना जोखिमों और कमजोरियों को कम करके कंप्यूटर सिस्टम और नेटवर्क को अनधिकृत पहुँच या अन्यथा क्षतिग्रस्त होने या दुर्गम होने से बचाने का अभ्यास है। सूचना जोखिमों में अनधिकृत पहुँच अवरोधन, उपयोग, प्रकटीकरण या डेटा विनाश शामिल हैं। साइबर सुरक्षा का उद्देश्य डेकर्स, स्पैमर्स और साइबर अपराधियों द्वारा किए गए।

E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

दुर्भावनापूर्ण हमलों से उपकरणों और सेवाओं की सुरक्षा के लिए एक बाल के रूप में कार्य करता है। संगठन फिटिंग योजनाओं, रॅनसमवेयर हमलों पहचान की चोरी, डेटा उल्लंघनों और संभावित वित्तीय नुकसान सहित विभिन्न खतरों से छुद को बचाने के लिऐ इस महत्वपूर्ण अभ्यास को अपनाते हैं। साइबर हमले का उद्देश्य संवेदनशील डेटा तक अनधिकृत पहुंच प्राप्त करना है। डेकर सिस्टम में घुसपैठ करने के लिए विभिन्न तकनीकों का उपयोग करते हैं, या तो महत्वपूर्ण डेटा को नष्ट करने या उसमें हेरफेर करने की कोशिश करते हैं। इस तरह की घुसपैठ के पीछे का मकसद अराजकता पैदा करने से लेकर रणनीतिक लाभ के लिए किसी साइबर सुरक्षा, सूचना जोखिमों और कमजोरियों को कम करके कंप्यूटर सिस्टम और नेटवर्क को अनधिकृत पहुँच या अन्यथा क्षतिग्रस्त होने या दुर्गम होने से बचाने का अभ्यास है। सूचना जोखिमों में अनधिकृत पहुँच अवरोधन, उपयोग, प्रकटीकरण या डेटा विनाशा शामिल हैं। साइबर सुरक्षा का उद्देश्य डेकर्स, स्पैमर्स और साइबर अपराधियों द्वारा किए गए कमजोरी का फायदा उठाना तक हो सकता है। कमी-कनी, साइबर अपराधी अवैध रूप से संवेदनशील जानकारी प्राप्त करके और पीड़ित को धमकाकर जबरन वसूली की रणनीति अपना सकते हैं। ये खतरे सूचना के प्रकटीकरण से लेकर फिरौती के बदले में डेटा डेरपोर तक हो सकते हैं। यह इमला संगठनों को अनिश्चित स्थिति में डालता है, जिससे इस तरह की बलपूर्वक कार्रवाई को रोकने के लिए मजबूत साइबर सुरक्षा उपायों की आवश्यकता पर बल मिलता है।

व्यवसाय तथा संस्थानों को नुकसान पहुंचानाः

डेकर्स व्यापार रहस्यों और बौद्धिक संपदा जैसी मूल्यवान जानकारी को निशाना बनाते हैं। उनका उद्देश्य वाली संपत्तियों को चुराकर और उजागर करके किसी प्रतिस्पर्धी के व्यवसाय को महत्वपूर्ण नुकसान पहुंचाना है। व्यापार रहस्यों को उजागर करने से प्रतिस्पर्धात्मक बढ़त खो सकती है, जिससे लाभप्रदता और बाजार की स्थिति प्रभावित हो सकती है। कुछ साइबर हमले किसी संगठन के नियमित संचालन को बाधित करने पर केंद्रित होते हैं। इसमें डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस इमले जैसी रणनीतियां शामिल हो सकती हैं, जिनका उद्देश्य सिस्टम और नेटवर्क को प्रभावित करना है। इसका उद्देश्य अराजकता पैदा करना, व्यावसायिक गतिविधियों में बाघा डालना और संभावित रूप से वित्तीय नुकसान पहुंचाना है। ऐसे विघटनकारी खतरों को कम करने के लिए साइबर सुरक्षा उपाय आवश्यक है। उल्लंघनों के कारण संगठन के ग्राहक आधार के बीच विश्वास की हानि होती है। आज के डिजिटल युग में साइबर सुरक्षा के महत्व को कम करके नहीं आंका जा

E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

सकता। आज की आपस में जुड़ी दुनिया में एक नी सुरक्षा उल्लंघन के गंभीर परिणाम होते हैं, जिसके परिणामस्वरूप नारी वित्तीय नुकसान और डेटा हानि होती है, साथ ही इसकी प्रतिष्ठा को भी नुकसान पहुंचता है। साइवर सुरक्षा का महत्व एवं विशेषताऐं साइबर सुरक्षा महत्वपूर्ण है क्योंकि यह संगठनात्मक परिसंपत्तियों और सेवाओं को दुर्भावनापूर्ण हमलों से बचाती है और सभी प्रकार के डेटा की सुरक्षा करती है, जिसमें संवेदनशील डेटा संरक्षित स्वास्थ्य सूचना (पीएचआई) और व्यक्तिगत रूप से पहचान योग्य जानकारी (पीआईआई) शामिल है, लेकिन यह चोरी और हानि तक सीमित नहीं है। साइबर सुरक्षा प्रमाणन प्राप्त करने से आपको घोखाघड़ी और ऑनलाइन हमलों से खुद को बचाने में मदद मिल सकती है! साइबर हमलों के कारण विनियामकों की ओर से जुर्माना लगाया जाता है और ग्राढक दावा करते हैं, जिसके परिणामस्वरूप बिक्री और राजस्य में कमी आती है, जिससे निरंतरता के महत्वपूर्ण पहलू प्रभावित होते हैं। इसके अतिरिक्त, साइबर अपराधा दैनिक संचालन को रोक सकते हैं। प्रौद्योगिकी के विकास के साथ, परिष्कृत हैकिंग पद्धतियां विकसित हुई हैं। आईटी टीम को साइबरस्पेस में तेजी से हो रहे बदलावों के साथ अपडेट रहना चाहिए। उपकरणों, तकनीकों और सहायता के साथ-साथ व्यापक ज्ञान से सुसज्जित एक कुशल आईटी टीम सबसे उन्नत साइबर अपराध को भी कुशलतापूर्वक संभाल सकती है। व्यक्तिगत डेटा व्यक्तियों और व्यवसाय मालिकों के लिए सबसे मूल्यवान संपत्तियों में से एक है। हालाँकि, मैलवेयर और वायरस आपकी व्यक्तिगत जानकारी तक पहुँच सकते हैं और कर्मचारियों, ग्राहकों या संगठनों की गोपनीयता को खतरे में डाल सकते हैं। साइबर सुरक्षा आंतरिक और बाहरी खतरों से डेटा की सुरक्षा करती है, चाहे ये आकस्मिक डों या दुर्भावनापूर्ण इरादे से, और कर्मचारियों को साइबर हमलों के खतरों के बिना आवश्यकतानुसार इंटरनेट तक पहुंचने में मदद करती है। जैसे-जैसे प्रौद्योगिकी विकसित हो रही है, साइबर अपराधी डेटा चोरी करने के लिए परिष्कृत तरीके अपना रहे हैं। वायरस नेटवर्क, वर्कपलो और कामकाज को प्रभावित करके उत्पादकता पर नकारात्मक प्रभाव डालते हैं। फर्म के डाउनटाइम के कारण संगठन टप्प पड़ सकता है। स्वचालित बैकअप और बेहतर फायरवॉल जैसे उपायों से फर्म अपनी उत्पादकता में सुधार कर सकती हैं, जो इसे साइबर सुरक्षा के सबसे आशाजनक लामों में से एक बनाता है। किसी भी गठन के लिएादक प्रतिवारण और ब्रांड निष्ठा बनाने में वर्षों लग जाते हैं। डेटा उल्लंघनों से व्यवसाय की प्रतिष्ठा को बहुत नुकसान पहुंचता है साइवर सुरक्षा प्रणाली के साथ संगठन अप्रत्याशित उल्लंघनों को कम कर सकते हैं। नेटवर्क सुरक्षा और क्लाउड सुरक्षा जैसी तकनीकें पहुँच और प्रमाणीकरण को मजबूत कर सकती हैं। इससे

E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

भविष्य की संस्तुतियों, उपक्रमों और विस्तारों के लिए मार्ग खुल सकता है। रिमोट वर्किंग मॉडल ने अलग-अलग स्थानों से काम करने वाले कर्मचारियों को अपने वर्कफलो के लिए कई रिमोट मॉडल तक पहुँचने के लिए प्रेरित किया है। संगठनों के लिए अपने संवेदनशील डेटा को दुनिया भर में प्रसारित करना परेशान करने वाला हो सकता है, जहाँ साइबर और सूचना सुरक्षा के खिलाफ अपराध व्यक्तिगत उपकरणों, उपकरणों, ब्लूटूथ, ४४ आदि जैसे चैनलों के माध्यम से हो सकते हैं। संवेदनशील डेटा, रणनीति और विश्लेषण हमेशा एक होने और लीक होने के प्रति संवेदनशील होते हैं। हालाँकि, साइवर सुरक्षा डेटा को संग्रहीत करने के लिए एक सुरक्षित केंद्र के रूप में कार्य करती है और घर के वाई-फाई को उपयोगकर्ताओं के डेटा को ट्रैक करने से भी बचा सकती है।

साइबर हमले व सुरक्षा नीति पहल

डाल के वर्षों में, कई व्यवसाय और व्यक्ति विनाशकारी परिणामों के साथ हाई प्रोफाइल साइबर हमलों का लक्ष्य रहे हैं। इनके परिणामस्वरूप सामाजिक सुरक्षा नंबर क्रेडिट कार्ड की जानकारी, बँक खाते के विवरण और संवेदनशील डेटा लीक की चोरी हो सकती है। इन हमलों ने संगठनों को मजबूत साइबर सुरक्षा उपायों के महत्व को समझने में मदद की है। निम्नलिखित साइबर हमलों के सबसे आम प्रकार हैं जिनका शिकार व्यक्ति और संगठन होते हैं मैलवेयर यह वायरस, ट्रोजन और वर्म्स जैसे सभी हानिकारक सॉफ्टवेयर को संदर्भित करता है जो कंप्यूटर सिस्टम को नुकसान पहुंचाने के इरादे से लिखा गया कोड या प्रोग्राम है। मैलवेयर कई प्रकार के होते हैं जैसे वायरस, वर्म्स, रैनसमवेयर, स्पाइवेयर एडवेयर और ट्रोजन।

वायरस : अपने जैविक समकक्षों की तरह, वे खुद को पुनः उत्पन करते हैं और उन्हें अन्य कंप्यूटरों में फैलाते हैं। ये फाइलों को दूषित कर सकते हैं, डेटा चुरा सकते हैं, या आपके कंप्यूटर को निष्क्रिय नी कर सकते हैं।

वस : वायरस की तरह, ये एक मशीन से दूसरी मशीन में फैल सकते हैं, लेकिन उन्हें खुद को दूसरी फाइलों से जोड़ने की जरूरत नहीं होती। तेजी से फैलने का कारण सॉफ्टवेयर से जुड़ी कमजोरियाँ हो सकती हैं।

ट्रोजन: असली होने का दिखाया करने वाले इन एप्लिकेशन को इंस्टॉल करने के बाद, ये आगे बढ़कर आपका डेटा चुरा लेंगे और अन्य मैलवेयर इंस्टॉल कर देंगे या आपकी मशीन को खराब कर देंगे।

E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

रैनसमवेयर: यह आपके दस्तावेजों को एन्क्रिप्ट कर देता है ताकि आप उन्हें दोबारा न देख सकें। इसके बाद हमलावर डिक्रिप्शन में इस्तेमाल की गई कुंजियों के बदले में फिरौती की मांग करते हैं।

स्पायवेयर इस प्रकार का सॉफ्टवेयर आपकी व्यक्तिगत जानकारी चुरा लेता है, जिसमें ब्राउजिंग इतिहास, लॉगिन क्रेडेंशियल और वित्तीय डेटा शामिल हैं। फिशिंगः इस तरह के सोशल इंजीनियरिंग हमलों में अवसर पीड़ितों को घोखा देकर उनकी निजी जानकारी का खुलासा किया जाता है। ये आम तौर पर ईमेल या टेक्स्ट संदेश भेजते हैं जो किसी शांत स्रोत से आए प्रतीत होते हैं, जैसे कि आप जिस बैंक से बैंकिंग कर रहे हैं या आपका कार्ड जारीकर्ता। ईमेल या टेक्स्ट में एक लिंक हो सकता है जो क्लिक करने पर एक प्रामाणिक वेबसाइट जैसा दिखता है। जब आप नकलीसाइट पर अपना विवरण दर्ज करते हैं, तो ये अपराधियों द्वारा चुरा लिए जाते हैं। इस तरह के हमले के दौरान, अपराधी आपके बैंक जैसे किसी अन्य व्यक्ति के साथ आपके संचार को सुन सकता है। इसके अलावा, यह आपकी व्यक्तिगत जानकारी भी चुरा सकता है।

सुरक्षा सायबर की पहल

·सायबर सुरक्षा नीति- इस निति का उददेश्य नगरिको व्यवसायों और

सरकार के लिए सुरक्षित और लचिला सायबर स्पेस बनाना यद सायवर

स्पेश की जानकारी और बुनियादी ढांचे की सुरक्षा सायबर हमलों को रोकने और उनका जवाब देने की क्षमता बनाने और संस्थागत संरचनाओं की रणनिति की रूपरेखा तैयार करता है।

· सायबर सुरक्षित भारत पहल- यह पहल सायबर अपराधों के बारे में जागरूकता बढ़ने और सभी सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों और अग्रीम पंवती के आईटी कर्मचारियों के लिए सुरक्षा उपाय बनाने के लिए शुरू की गई थी।

· कम्प्यूटर आपातकारी प्रतिक्रिया टीमः- यह इलेक्ट्रोनिक सूचना प्रौद्योगिकी मंत्रालय का एक संगठन है जो सायवर घटनाओं पर सूचना एकत्रित विश्लेषण और प्रसार करता है सायबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।

E-ISSN No: 2456-6713 Print ISSN No: 3048-6459

International Educational Applied Research Journal

Peer-Reviewed Journal-Equivalent to UGC Approved Journal

A Multi-Disciplinary Research Journal

निष्कर्ष

भारत को सरकारी और निजी क्षेत्र के प्रतिभागियों के साथ एक सायबर सुरक्षा बोर्ड की सुरक्षा करनी चाहिए जिसके पास किसी महत्वपूर्ण सायबर घटना के बाद बैठक आयोजित करने घटित घटना का विश्लेषण करने और सायबर सुरक्षा सुधार के लिए दोस सिफारिस करने का अधिकार हो ।

सायबर सुरक्षा की चुनौतियों का सामना करने में भारत अकेला नहीं क्योकि सायबर हमले राष्ट्रीय सीमा को पार करते है और वैश्विक समुदाय को प्रभावित करते हैं। भारत को क्षेत्रीय और द्विपक्षीय वार्ताओं और पहलूओं में अधिक सक्रियता से भाग लेने की आवश्यकता है जैसे कि आसियान क्षेत्रीय मंच, ब्रिक्स और भारत अमेरिका सायबर सुरक्षा मंच जैसे द्विपीक्षय मंच ताकि विश्वास और आत्मविश्वास का निर्माण हो सके।

संदर्भ:-

1. **टाइम्स ऑफ इण्डिया**

2. **सायबर सिक्योरिटी (बी.सिंह)**

3. **ईन्टरनेट विधि एवं सायबर अपराध (तलत फातिमा)**

4. **भारत में सायबर अपराध (डॉ. ललित कुमार)**