डेटासेंटर और इसके सुरक्षा उपाय
(Datacenters and Its Security Measures)

अंजलि होरा[1], सारिका जैन[2], विशाल लामा[3]
(Anjali Hora[1], Sarika Jain[2], Vishal Lama[3])

[1]National Institute of Technology, Kurukshetra, Haryana, India
[1]horaanjali@gmail.com [2]jasarika@gmail.com [3]lama.vishal94@gmal.com

Abstract

डेटासेंटर गूगल, अमेज़ॅन, माइक्रोसॉफ्ट, फेसबुक जैसी कुछ सबसे बड़ीआईटी कंपनियों के लिए ईंधन हैं।इन कंपनियों द्वारा विकसित तकनीकें इन डेटासेंटर का उपयोग करती हैं।इतना ही नहीं, ये कंपनियां अपने सेवाओं को बेचकर छोटे व्यवसायों की मदद कर रही है जो डेटासेंटर पर निर्भर हैं।यह चर्चा के लिए एक महत्वपूर्ण विषय बन रहा है क्योंकि प्रत्येक निर्णय अब संसाधित रूप में बड़ी मात्रा में डेटा पर भरोसा कर रहा है जो डेटासेंटर में निहित रूप से संग्रहीत है।डेटासेंटर इन बड़े पैमाने पर उद्यमों के लिएअभिन्न अंग हैं क्योंकि बढ़ती मांग का जवाब देने के लिए इसमें स्केल करने की क्षमता है।हमारे कंप्यूटर आर्किटेक्चर के कुछ हिस्सों को स्केल करना आमतौर पर कंप्यूटिंग क्षमता, स्मृति, नेटवर्किंग आधार भूतसंरचना, या भंडार संसाधनों में वृद्धि का मतलब है।प्रौद्योगिकी में प्रगति के साथ, डेटासेंटर को सुरक्षित रखना प्रमुख चिंता है।यह पेपर डेटासेंटरऔर इसके प्रभाव से संबंधित है।इसकेअलावा, पेपर डेटासेंटर को सुरक्षित करने के लिए समाधान प्रदान करता है।

कीवर्ड: डेटासेंटर; सेशन हाईजैकिंग; फ़िशिंग; सोशल इंजीनियरिंग; सर्विस लेवल एग्रीमेंट

1. डाटासेंटर

डिजिटलीकरण के बढ़ने से लोग टेक्नोलॉजी पर भरोसा कर रहे है। जिस तरह ग्राहक के लिए उसका डाटा महत्वपूर्ण है उसी प्रकार उसी डाटा को सुरक्षित रूप से स्टोर करना भी महत्वपूर्ण है। यह डेटा ग्राहकों द्वारा मांग की पूर्ति के लिए कंपनियों द्वारा उठाए गए कई बड़े निर्णय लेने के आधार बनते है और इसके साथ ही वे अपना स्वयं का राजस्व उत्पन्न करते हैं। भारतीयकरण भारतीय रिजर्व बैंक (भारतीयरिज़र्वबैंक) द्वारा अधिसूचित किया गया है कि डाटा की भुगतान प्रणाली से संबंधित डेटा भारत के भीतर स्थित होना चाहिए जो लोकलाइजेशन की आवश्यकता बताते है । यह ग्राहक के डेटा को सुरक्षित करने और भारत में उपयोग कर्ताओं के लिए पहुंच की गति बढ़ाने के लिए एक पहल है।एनटीपी (नेशनलटेलीकॉमपॉलिसी) 2018 के प्रावधान के तहत, सरकार दूरसंचार सेवा प्रदाता ओंसेयह सुनिश्चित करने के लिए कह सकती है कि भारतीय नागरिकों के संदेश, ईमेल इत्यादि देश के सीमाओं के भीतर रखे जाएं जबतक कि विदेशों में रहने वाले लोगों को संबोधित नकिया जाए। एनटीपी 2022 तक स्थानीय नागरिकों में रखे जाने वाले भारतीय नागरिकों और संस्थाओं के डेटा होस्ट करने वाले सभी सर्वरों की स्थापना का प्रस्ताव दे सकता है।

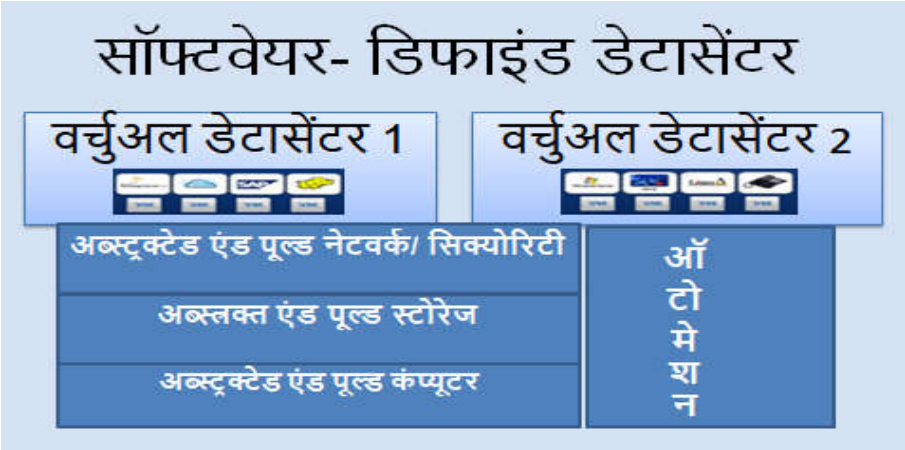
पारंपरिक डाटासेंटर (सिलेड) जो कि हार्डवेयर और फिजिकल सर्वर पर भारी निर्भर करता है, इससे स्टोरेज स्पेस पर सीमा हो सकती है।जितना अधिक स्पेस होगा उतना ही हार्डवेयर और फिजिकल सर्वरों कीआवश्यकता होगी। धीमी और इनएफ़फीसिएंट डिलीवरी एक और प्रमुख चुनौती थी। संसाधनों का उपयोग उन प्रमुख नुकसानों में से एक हो सकता है जो नए अनुप्रयोगों को तैनात करने में महीनों लगा रहा हैं।इन नुकसानों के साथ, वर्चुअलाइज्ड डेटासेंटर के बारे में आया क्योंकि वर्चुअल टेक्नोलॉजी क्रांति में चुने गए डेटासेंटर से कंप्यूटिंग, नेटवर्क और स्टोरेज के संसाधनों को पूल

करना संभव बना दिया ताकि एक केंद्रीय, अधिक लचीला संसाधन बनाया जा सके जो जरूरतों केआधार पर फिर सेआवंटित किया जा सके।आज लगभग हर संगठन में कम से कम 25 प्रतिशत वर्चुअल डेटा वाले डेटासेंटर हैं।

असंगठित रूप में डेटा के बड़े हिस्से को संग्रहित करने के अलावा, संसाधन कें द्रोंका उपयोग उन संसाधनों के बेहतर उपयोग के लिए किया जाना था जहां आवेदन उन्हें कुशलता से उपयोग कर सकते हैं।सर्वर वर्चुअलाइजेशन पूल में संसाधनों को साझा करने पर आधारित था।आवश्यक होने पर पूल में उपलब्ध संसाधनों का उपयोग किया जा रहा है। इस्तेमाल होने पर, इन संसाधनों को फिर से पूल में रखा जाता है।समस्या उत्पन्न होती है जब एक एप्लिकेशन संसाधनों पर निर्भर करती है जोकि दूसरी एप्लीकेशन की भी ज़रूरत है जिसकी वजह से संसाधनों की कमी की वजह बन जाती है ।यह वह जगह है जहां सर्विस लेवल एग्रीमेंट टूट जाता है।सर्विस लेवल एग्रीमेंट सर्वरुप्टिमेस 100% के करीब और संसाधनों की उपलब्धता की गारंटी देता है।

आज के कारोबार के इस तरह के एक गतिशील वर्क लोड को प्रबंधित करने के लिए, एस एल आई (स्केलेबल लिंक इंटरफ़ेस है, जो वर्तमान वर्कलोड की मांगों के आधार पर अपनी क्षमता को कम कर सकता है और विस्तार कर सकता है)।

व्यापारिक दुनिया में जटिलताओं को देखकर, एंटरप्राइज़ आर्किटेक्चर मौजूदा लोड के लिए सिस्टम को ऑप्टिमाइज़ करने सेअधिक लचीला वातावरण की नींव बनाने के लिए स्थानांतरित हो रहा है जिसे बिना किसीआधार भूतसंरचना पुन र्निर्माण के पुनः डिजाइन और पुनर्गठित किया जा सकता है।



डायग्राम 1. डायग्राम मे दिखाया गया है की कैसे संसाधनों को पूल किया जा रहा है दो वर्चुअल डाटा सेंटर का उपयोग कर।

2. डेटासेंटर् पर अटैक

डाटासेंटर का निर्माण आई टी फर्मों द्वारा किया जाता है।यह न केवल डेटास्टोर करता है बल्कि संसाधनों तक बेहतर पहुंच प्रदान करता है। सिनफुलनॉक जैसे टूल हैं, जो दिखाते हैं कि हैकर्स नेटवर्क में अन्य राउटर को उसी नेटवर्क में एक राउटर के नियंत्रण प्राप्त करके नियंत्रित करते हैं।

एक सर्वर या डेटासेंटर पर हमले समान हैं लेकिन किसी व्यक्ति या उद्यम के संबंध में स्तर अलग है। सूक्ष्म हमलावर उन दरों पर डेटा को धैर्य पूर्वक बहिष्कृत करके कम और धीमी रहने का प्रयास कर सकते हैं जिनपर कम ध्यान देने की संभावना है या संदेह उत्पन्न होता है। वेबयाडी.न.सयातायात जैसे अनुमत ट्रैफ़िक के भीतर छिपे सुरंगों में डेटा एक्सफिल्टरेशन कोअस्पष्ट करने के प्रयास भी किए जा सकते हैं।

डेटा कें द्रोंपर हमले निम्नानुसार हैं:

2.1 सेशन हाईजैकिंग

सेशन हाईजैकिंग एक प्रमाणित सेशन आई डी प्राप्त करने के बाद उपयोग कर्ता सत्र पर नियंत्रण लेने का कार्य है।

सेशन हाईजैकिंग के स्टेप्स-

•विक्टिम और लक्ष्य के बीच खुद को रखें (आप नेटवर्क को स्निफ्फ करने में सक्षम होने चाहिए)

•पैकेट के प्रवाह की निगरानी करें

•सीक्वेंस नंबर की भविष्यवाणी करें

•विक्टिम की मशीन से कनेक्शन को मार डालो

•सेशन को टेक ओवर करना

•टारगेट सर्वर पर पैकेट इंजेक्शन शुरू करें

2.2 फ़िशिंग

फ़िशिंग नकली संचार भेजने का अभ्यास है जो एक प्रतिष्ठित स्रोत से आती है और आमतौर पर ई-मेल के रूप में दिखाई देती है। क्रेडिटकार्ड और लॉगिन जानकारी जैसे संवेदनशील डेटा चुराना या पीड़ित की मशीन पर मैलवेयर इंस्टॉल करना फिशिंग का लक्ष्य है।

2.2.1 डी.ऍ.एस -आधारित फ़िशिंग आपके होस्ट फ़ाइलों या डोमेन नामों से समझौता करती है और अपने व्यक्तिगत या भुगतानविवरण दर्ज करने के लिए अपने ग्राहकों को झूठे वेबपृष्ठ पर निर्देशित करती है।

2.1.2 कंटेंट-इंजेक्शन फ़िशिंग आपके कर्मचारियों और लॉगिन विवरण जैसे ग्राहकों से व्यक्तिगत जानकारी कैप्चर करने से जुड़ी है।इस प्रकार की फ़िशिंग अक्सर उन व्यक्तियों को लक्षित करती है जो विभिन्न वेबसाइटों पर एक ही पासवर्ड का उपयोग करते हैं।

2.1.3 मैन-इन-द-मिडिल फ़िशिंग में अपराधियों को आपकी कंपनी की वेबसाइट और आपके ग्राहक के बीच रखने का अधिकार शामिल है।इससे उन्हें आपके ग्राहक द्वारा दर्ज की जाने वाली सारी जानकारी कैप्चर करने की अनुमति मिलती है, जैसे व्यक्तिगत जानकारी और क्रेडिटकार्ड विवरण।

2.3 सोशल इंजीनियरिंग

यह एक कर्मचारी को प्रशासक प्रमाण-पत्र प्राप्त करने और इसका दुरुपयोग करने के लिए एक तकनीक है।

2.4 डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस

एक डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस (डी डी ओ एस) हमला एक या अधिक लक्ष्यों के खिलाफ एक समन्वित डॉस हमले लॉन्च करने के लिए कई कंप्यूटरों का उपयोग करता है।डॉस सेवा के हमले के अस्वीकार के लिए संक्षिप्त नाम है।यह कंप्यूटर या नेटवर्क पर हमला है जो वैधउपयोगकर्ताओं द्वारा अपने संसाधनों का उपयोग रोकता है।डी डी ओ एस हमले में तेजी से वृद्धि के साथ, 2011 और 2013 के बीच डी डी ओ एस हमलों का औसत आकार 4.7 से 10 जीबीपीएस तक बढ़ता है।

3. सुरक्षा उपाय

संदिग्ध अनुलग्नकों को फ़िल्टर करने और दुर्भावनापूर्ण यूआरएल पर फ़िल्टर करने की अनुशंसा की जाती है। अच्छे प्रमाण पत्र व्यवहार को बढ़ावा देना जैसे कमजोर पासवर्ड को अस्वीकार करना या उपयोगकर्ताओं के लिए पुनरावर्ती पासवर्ड परिवर्तन लागू करना इस मुद्दे को भी रोक देगा। इंटरनेट पर व्यक्तिगत जानकारी संचारित करने से पहले, कनेक्शन सुरक्षित है और जांचें कि यूआरएल सही है। यदि कोई ईमेल संदेश वैध है तो अनिश्चित है, सत्यापित करने के लिए किसी अन्य माध्यम से व्यक्ति या कंपनी से संपर्क करें। एंटी-वायरस और फ़ायरवॉल स्थापित करना डेटा सेंटर्स को रोकने के लिए एक और विकल्प है। ईमेल फ़िल्टर लागू करने से अवांछित यातायात का प्रबंधन करने में मदद मिल सकती है।

कर्मचारी को शिक्षित करना महत्वपूर्ण है। कर्मचारियों को नियमित सुरक्षा प्रशिक्षण उन्हें फिशिंग स्कैन, मैलवेयर और सोशल इंजीनियरिग खतरों की पहचान करने में मदद कर सकता है। सभी प्रणालियों पर नवीनतम सुरक्षा पैच और अपडेट डेटा सेंटर्स की सुरक्षा के लिए एक अच्छा तरीका है।

संवेदनशील कंपनी की जानकारी की रक्षा करने के लिए एन्क्रिप्शन एक और तकनीक है। एचटीएमएल ईमेल संदेशों को अक्षम करने से आपके सिस्टम की सुरक्षा में मदद मिल सकती है क्योंकि ये स्क्रिप्टिंग फ़ाइल एक दुर्भावनापूर्ण कोड हो सकती है जिसे जानबूझकर सिस्टम में जोड़ा जाता है।

मूलभूत जानकारी जैसे कि यूआरएल की सावधानीपूर्वक पढ़ने, पासवर्ड को मजबूत रखने, अजनबियों या धोखाधड़ी करने वाली वेबसाइटों को पासवर्ड और खाता जानकारी प्रकट करने से उपयोगकर्ता की मदद भी मिल सकती है।

एसएसएल प्रमाणपत्र आपकी वेबसाइट पर सभी ट्रैफ़िक सुरक्षित करने में मदद करता है। यह वेब सर्वर और ग्राहक के ब्राउज़र के बीच सहेजी गई जानकारी को सहेजने से बचाता है। आवेदन वितरण नियंत्रक (एडीसी) संगठनों को उनके डेटा सेंटर आधारभूत संरचना की सुरक्षा के लिए सहायता करते हैं।इसमें निम्नलिखित विशेषताएं हैं:

•एन्क्रिप्टेड यातायात का निरीक्षण करें
•अनुप्रयोगों में अनधिकृत पहुंचको रोकें
•डी डी ओ एस सुरक्षा
•वेब एप्लीकेशन फ़ायरवॉल (डब्ल्यूएएफ)
•डी.ऍन.एस एप्लीकेशन फ़ायरवॉल (डीएएफ)
•एसएसएल अंतर्दृष्टि
•एसएसएल ऑफलोड

4. निष्कर्ष

डाटासेंटर उद्यमों के लिए रीढ़ की हड्डी हैं।यह इतना महत्वपूर्ण हो रहा है कि इसे और भी मजबूत बनाने के लिए नई तकनीकें लागू की जा रही हैं। हाइपरस्केल कंप्यूटिंग उन तकनीकों में से एक है। इस पेपर का उद्देश्य कुछ सुरक्षा उपाय प्रदान करके डेटासेंटर को रोकने के लिए है। पेपर पहले डेटासेंटर के बारे में वर्णन करेगा, और फिर गंभीर हमले जो हैकर डेटासेंटर के ऊपर कर रहे है उसके बारे मे बताया है ।इस पेपर के अंत में, समाधान दिए जाते हैं जो डेटासेंटर को हैकर्स द्वारा हमला करने से रोक सकते हैं।

संदर्भ

1. Kaufman, Lori M. "Data security in the world of cloud computing." IEEE Security & Privacy 7.4 (2009).
2. Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." Information Security for South Africa (ISSA), 2010. IEEE, 2010.
3. Al-Fares, Mohammad, Alexander Loukissas, and Amin Vahdat. "A scalable, commodity data center network architecture." ACM SIGCOMM Computer Communication Review. Vol. 38. No. 4. ACM, 2008.
4. Greenberg, Albert, et al. "VL2: a scalable and flexible data center network." ACM SIGCOMM computer communication review. Vol. 39. No. 4. ACM, 2009.
5. Greenberg, Albert, et al. "The cost of a cloud: research problems in data center networks." ACM SIGCOMM computer communication review 39.1 (2008): 68-73.
6. Kandula, Srikanth, et al. "The nature of data center traffic: measurements & analysis." Proceedings of the 9th ACM SIGCOMM conference on Internet measurement. ACM, 2009.
7. Alizadeh, Mohammad, et al. "Data center tcp (dctcp)." ACM SIGCOMM computer communication review 41.4 (2011): 63-74.