अमेरिकी वायुसेना के 'क्लाउड वन' में साइबर घुसपैठ: संवेदनशील सैन्य डेटा पर खतरा

समाचार-संदर्भ: 27 नवंबर 2026

प्रकाशन: 28 नवंबर 2026

मुख्य परीक्षा: GS-III, साइबर सुरक्षा और सैन्य डिजिटल ढाँचा



मौलिक प्रतीकात्मक चित्र: pcsmantra.com

▼ इस लेख में

1. खबरों में क्यों
2. रिपोर्ट की मुख्य बातें
3. क्लाउड वन क्या है
4. असर कहाँ-कहाँ दिखा
5. बड़ा संदर्भ
6. परीक्षा की दृष्टि से विश्लेषण
7. आगे की राह
8. मुख्य परीक्षा अभ्यास प्रश्न
9. स्रोत
10. अक्सर पूछे जाने वाले प्रश्न

खबरों में क्यों

समाचार एजेंसी रॉयटर्स की 27 नवंबर 2026 की रिपोर्ट के अनुसार अमेरिकी वायुसेना के प्रमुख क्लाउड कंप्यूटिंग मंच 'क्लाउड वन' (Cloud One) में हैकर्स घुस आए हैं। रिपोर्ट में मामले की जानकारी रखने वाले तीन सूत्रों के हवाले से कहा गया है कि इससे संवेदनशील सामरिक, कार्मिक और रसद डेटा खतरे में पड़ सकता है। [1]

रिपोर्ट की मुख्य बातें

मूल बात समझिए: क्लाउड कंप्यूटिंग का अर्थ है अपने कंप्यूटर के बजाय इंटरनेट पर स्थित सर्वरों से डेटा और सेवाएँ लेना। क्लाउड वन अमेरिकी वायुसेना का केंद्रीय मंच है, जहाँ उसके कई महत्वपूर्ण ऐप चलते हैं।

घुसपैठ कैसे पता चली: रिपोर्ट के अनुसार सिस्टम को अपग्रेड करने के काम के दौरान, बीते महीने के भीतर, घुसपैठ का पता चला। इसके बाद मंच पर काम बाधित हुआ। [1]

क्या पता नहीं चल सका: हैकर्स कौन हैं, घुसपैठ कितनी गहरी है और कोई डेटा चोरी हुआ या नहीं, रिपोर्ट इसकी पुष्टि नहीं कर सकी। अमेरिकी वायुसेना ने कहा कि वह विशिष्ट नेटवर्क की सुरक्षा स्थिति, कमजोरियों या परिचालन हालात पर टिप्पणी नहीं करती, और सूचना-तंत्र की सुरक्षा के लिए निरंतर उचित कदम उठाए जाते हैं। [1]

जांच कौन कर रहा है: रिपोर्ट के अनुसार अमेरिकी सेना की साइबर बल, साइबर कमांड (Cyber Command) को नुकसान का आकलन के लिए बुलाया गया है।

क्लाउड वन क्या है

शुरुआत: वर्ष 2017 में शुरू यह मंच वायुसेना की सूचना-तकनीक ज़रूरतों का 'वन-स्टॉप शॉप' (एक ही जगह सारी सुविधा) बनाया गया। [1]

कौन चलाता है: इसमें चार तकनीकी कंपनियों, माइक्रोसॉफ्ट, अमेज़न, ओरेकल और अल्फाबेट (गूगल की मूल कंपनी) के संसाधन एक साथ जुड़े हैं। ठेका 2026 तक SAIC के पास था, इसके बाद Leidos को मिला। [1]

कौन-से ऐप: इसी मंच पर कार्मिक डेटा और वेतन, रसद और रखरखाव जैसे कई ऐप चलते हैं। इनमें क्लाउड-आधारित कमांड एंड कंट्रोल सिस्टम है, जो उत्तरी अमेरिका भर के वायु-रक्षा रडार डेटा जुटाता है, और थिएटर इंटीग्रेटेड कॉम्बैट म्युनिशंस सिस्टम, जो दुनिया भर के 200 से अधिक वायुसेना ठिकानों पर बम-मिसाइलों का हिसाब रखता है। रिपोर्ट के अनुसार यह अमेरिकी सेना के सबसे बड़े क्लाउड मंचों में है। [1]

असर कहाँ-कहाँ दिखा

माइग्रेशन रुका: पुराने (बैक-ऑफिस) ऐप को क्लाउड वन पर लाने का काम रोक दिया गया।

अपडेट बंद: पहले से चल रहे ऐप के अपडेट भी ब्लॉक कर दिए गए, जबकि तकनीकी क्षेत्र में उसी दौरान कई गंभीर सॉफ्टवेयर कमजोरियाँ सामने आई हैं।

अधिकार वापस: कुछ उपयोगकर्ताओं के प्रशासक (एडमिन) अधिकार वापस लिए गए।

कंट्रोल प्लेन तक पहुंच: एक सूत्र के अनुसार घुसपैठियों ने सॉफ्टवेयर की कमजोरी का फायदा उठाकर 'कंट्रोल प्लेन' (नियंत्रण स्तर) तक पहुंच बनाई। कंट्रोल प्लेन वह केंद्रीय परत है जो पूरे मंच को चलाती है; रिपोर्ट इसे सार्वभौमिक रिमोट जैसा बताती है, जिससे सिद्धांततः विमानों की परिचालन स्थिति या पुरजों की आवाजाही देखी जा सकती है, हालांकि ऐसा हुआ या नहीं, यह स्पष्ट नहीं है। [1]

बड़ा संदर्भ

हमलों की लहर: रिपोर्ट के अनुसार अमेरिकी सरकार हाल में सामने आई कम-से-कम छह और साइबर घटनाओं से जूझ रही है। इनमें FBI से जुड़ी दो घटनाएँ, पेंटागन के डेटा में पुरानी घुसपैठ, गृह सुरक्षा विभाग के कार्मिकों की जानकारी का लीक होना, कम-से-कम दो खुफिया एजेंसियों को प्रभावित करने वाली घुसपैठ और खजाना विभाग में हैक शामिल हैं। [1]

AI से तेज हमले: आर्टिफिशियल इंटेलिजेंस (AI) से चलने वाले हमलों की चिंता बढ़ी है, क्योंकि AI मॉडल बड़े नेटवर्क में कमजोरियाँ तेजी से ढूँढ सकते हैं। क्लाउड-आधारित नेटवर्क पर यह जोखिम खास है।

पुराना दावा: क्लाउड वन प्रबंधन ने वर्ष 2023 में एक टिप्पणी में दावा किया था कि मंच में घुसने के "चौंकाने वाली संख्या" में प्रयासों को "100% सफलता" से रोका गया। रिपोर्ट में यह भी कहा गया है कि सुरक्षा के मामले में "गलती की गुंजाइश नहीं" है। [1]

परीक्षा की दृष्टि से विश्लेषण

एक मंच पर सब कुछ = एकल विफलता बिंदु: जब कई संवेदनशील प्रणालियाँ एक ही क्लाउड मंच पर होती हैं, तो एक ही घुसपैठ व्यापक असर डाल सकती है। साझा क्लाउड लागत और प्रबंधन घटाता है, पर केंद्रीकरण जोखिम भी बढ़ाता है।

शून्य-विश्वास (zero-trust) की ज़रूरत: इस मॉडल में हर उपयोगकर्ता और हर सत्र की बार-बार जांच होती है, भरोसा पहले से नहीं माना जाता। इस घटना से स्पष्ट है कि केवल परिधि-सुरक्षा पर्याप्त नहीं।

AI युग की चुनौती: AI से हमले की गति और पैमाना बढ़ता है, इसलिए पहचान और प्रतिक्रिया भी स्वचालित करनी होगी। भारत के लिए सीख: महत्वपूर्ण बुनियादी ढाँचे की सुरक्षा में राष्ट्रीय साइबर सुरक्षा रणनीति और CERT-In जैसी एजेंसियों की भूमिका और सतर्कता।

सीमा: यह पूरी खबर गुमनाम सूत्रों पर आधारित एक ही रिपोर्ट है। आधिकारिक पुष्टि न होने से निष्कर्ष सावधानी से निकालने होंगे; अंतिम तथ्य जांच के बाद ही पता चलेंगे।

आगे की राह

घुसपैठ की पूरी जांच, प्रभावित प्रणालियों का अलगाव (सेगमेंटेशन) और आपूर्ति-शृंखला (कंपनियों और सॉफ्टवेयर) की बारीक जांच ज़रूरी होगी। दीर्घकाल में महत्वपूर्ण सैन्य प्रणालियों के लिए शून्य-विश्वास ढाँचा, निरंतर निगरानी और घटना-प्रतिक्रिया की तैयारी पर जोर रहने की उम्मीद है।

मुख्य परीक्षा अभ्यास प्रश्न

प्रश्न 1. "क्लाउड-आधारित रक्षा संचालन सामरिक सुविधा तो देते हैं, पर साइबर जोखिम को भी केंद्रीकृत कर देते हैं।" अमेरिकी वायुसेना की क्लाउड वन घुसपैठ के संदर्भ में इस कथन की समीक्षा कीजिए और भारत के लिए सीख सुझाइए। (250 शब्द, 15 अंक)

▼ उत्तर और व्याख्या

भूमिका में: क्लाउड वन घुसपैठ की रिपोर्ट का संक्षिप्त परिचय: क्या हुआ, क्या पुष्ट नहीं हुआ।

मुख्य भाग में: क्लाउड के लाभ (एकीकृत संसाधन, लागत, तेज अपडेट) बनाम एकल विफलता बिंदु और कंट्रोल प्लेन तक पहुंच का जोखिम; गुमनाम सूत्रों वाली रिपोर्ट की सीमा; AI-संचालित हमलों की बढ़ती चुनौती; शून्य-विश्वास ढाँचा, सेगमेंटेशन और आपूर्ति-शृंखला सुरक्षा; भारत के लिए सीख: महत्वपूर्ण बुनियादी ढाँचे की सुरक्षा और CERT-In की भूमिका।

निष्कर्ष में: संतुलित निष्कर्ष: क्लाउड अपरिहार्य है, पर सुरक्षा को डिज़ाइन का हिस्सा बनाना होगा, बाद में जोड़ा हुआ उपाय नहीं।

स्रोत

- [1] https://www.cnbc.com/2026/11/27/hackers-breach-us-air-force-flagship-cloud-one-computing-platform.html

अक्सर पूछे जाने वाले प्रश्न

क्लाउड वन क्या है?

यह अमेरिकी वायुसेना का प्रमुख क्लाउड कंप्यूटिंग मंच है, जो 2017 में शुरू हुआ। इसमें माइक्रोसॉफ्ट, अमेज़न, ओरेकल और अल्फाबेट के संसाधन जुड़े हैं और वेतन, रसद और कमांड-नियंत्रण जैसे कई ऐप इसी पर चलते हैं।

क्या हैकर्स की पहचान या डेटा-चोरी की पुष्टि हुई?

नहीं। रिपोर्ट गुमनाम सूत्रों पर आधारित है और हैकर्स की पहचान, घुसपैठ का पूरा दायरा या डेटा-चोरी की पुष्टि नहीं कर सकी। अमेरिकी वायुसेना ने विशिष्ट नेटवर्क की सुरक्षा स्थिति पर टिप्पणी से इनकार किया है।

PCSMANTRA.COM

कंट्रोल प्लेन क्या होता है?

यह क्लाउड मंच की केंद्रीय नियंत्रण परत है, जो पूरे सिस्टम के संचालन को निर्देशित करती है। इस तक पहुंच मिलने पर सिद्धांततः कई प्रणालियों की स्थिति देखी या प्रभावित की जा सकती है।

यह घटना भारत के लिए क्यों महत्वपूर्ण है?

यह दिखाती है कि महत्वपूर्ण रक्षा-प्रणालियों को एक मंच पर केंद्रीकृत करने से जोखिम बढ़ता है। भारत के लिए शून्य-विश्वास सुरक्षा, निरंतर निगरानी और CERT-In जैसी संस्थाओं की तैयारी की सीख है।

PCSMANTRA.COM