कार्यकारी सारांश

साइबर-सुरक्षा मिथक:

इंक्रीमेंटल फिक्स क्यों नाकाफ़ी होते हैं—और EzIP एक आसान, ज़्यादा सुरक्षित रास्ता क्यों देता है

इंटरनेट आधुनिक समाज को पावर देता है, फिर भी वह कमज़ोर बना हुआ है। क्लाउडफ्लेयर (नवंबर 2025) में हाल ही में हुए ग्लोबल आउटेज और Amazon Web Services में बार-बार होने वाली रुकावटें लगातार कमज़ोरी को उजागर करती हैं, यहाँ तक कि टॉप प्रोवाइडर्स के बीच भी जिन्हें सुरक्षा और विश्वसनीयता बढ़ाने के लिए डिज़ाइन किया गया है। फेडरल प्रयास (FCC NPRM, 2024) और व्हाइट हाउस के इंटरनेट routing सुरक्षा बढ़ाने के रोडमैप (2024) बॉर्डर गेटवे प्रोटोकॉल (BGP) को मज़बूत मॉनिटरिंग और वैलिडेशन के लिए टारगेट करते हैं। ये कदम उपयोगी हैं लेकिन एक गहरी समस्या के लक्षणों को संबोधित करते हैं: IPv4 एड्रेस की मूल कमी। सीमित एड्रेस से निपटने के लिए:

- • डायनामिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल (DHCP) ने IP एड्रेस को टेम्परेरी बना दिया।
- • DNS ने बदलावों को ट्रैक किया।
- • नेटवर्क हज़ारों डोमेन (ऑटोनॉमस सिस्टम) में बंट गए, जिन्हें जोड़ने के लिए BGP पर निर्भर रहना पड़ा।
- • कंटेंट डिलीवरी नेटवर्क (CDN) ने कॉम्प्लेक्सिटी को मैनेज करने के लिए ट्रैफ़िक को सेंट्रलाइज़ किया।

हर स्टेप कन्फ्यूजन, सिंगल पॉइंट्स ऑफ़ फेलियर और हमलावरों को फ़ायदा पहुंचाता है। स्पूफ किए गए एड्रेस इंस्टॉल करने में आसान होते हैं और उन्हें ट्रेस करना मुश्किल होता है, जबकि वैलिड यूज़र्स सही रिकॉर्ड छोड़ जाते हैं। सेंट्रलाइज़्ड CDN मुख्य टारगेट बन जाते हैं, और पैचिंग रूट कारण को हल किए बिना और लेयर्स जोड़ देती है। EzIP (इज़ी IPv4) लंबे समय से रिज़र्व किए गए IPv4 240/4 ब्लॉक को फिर से इस्तेमाल करके इस समस्या को ठीक करता है ताकि लाखों जगहों को यूनिक, स्टैटिक पब्लिक एड्रेस दिए जा सकें - जो पूरे क्षेत्रों को बिना डायनामिक रीसाइनमेंट के। प्रॉब्लम वाले प्रोटोकॉल पर ज़्यादा निर्भरता को सर्विस देने के लिए काफ़ी हैं। मुख्य फ़ायदे:

• ज़्यादा मज़बूत इनहेरेंट सिक्योरिटी — स्टैटिक एड्रेस स्पूफिंग का पता लगाना आसान बनाते हैं, ट्रेसेबिलिटी बेहतर करते हैं, और डिज़ाइन के हिसाब से सही टेक सरफेस को कम करते हैं।
• ज़्यादा विश्वसनीयता — कम जटिलता से आउटेज का जोखिम कम होता है; सटीक जियो-लोकेशन मैनेजमेंट और रिस्पॉन्स में मदद करता है।
• कम से कम रुकावट — मौजूदा इंटरनेट पर ओवरले करता है; बेहतर रीजनल राउटर के ज़रिए धीरे-धीरे डिप्लॉय होता है; बड़े पैमाने पर डिवाइस पैच की ज़रूरत नहीं है।
• व्यापक फ़ायदे — सेंट्रलाइज़ेशन के जोखिमों को कम करता है; इंटरनेट आर्किटेक्चर को बेहतर बनाता है; बेहतर कानून प्रवर्तन एट्रिब्यूशन को सपोर्ट करता है।

EzIP, IPv6 और मौजूदा टूल्स को कॉम्प्लिमेंट करता है, जो इंटरनेट को कमजोर बनाने वाली बुनियादी कमी को दूर करता है। यह ज़्यादा मज़बूत, न्यायसंगत डिजिटल इंफ्रास्ट्रक्चर के लक्ष्यों का समर्थन करता है। पूरी एनालिसिस के लिए, कृपया यहाँ जाएँ:

https://avinta.com/gallery/CyberSecurityMyth-IN.pdf

द्वारा तैयार: Abraham Y. Chen / Avinta Communications, Inc.
संपर्क करें: AYChen@Avinta.com / +1(650)248-1829
2026 जनवरी