माइक्रोसफ्टको त्रुटिले एआई उपकरण कोपाइलटमा गोप्य इमेलहरू पर्दाफास भएको देखाउँछ

२ दिन अगाडि

लिभ म्याकमोहन
प्रविधि रिपोर्टर

गेट्टी चित्रहरू

माइक्रोसफ्टले आफ्नो एआई कार्य सहायकले गल्तीले केही प्रयोगकर्ताहरूको गोप्य इमेलहरू पहुँच गर्न र सारांशित गर्न त्रुटि भएको स्वीकार गरेको छ।

टेक जायन्टले कार्यस्थलहरू र उनीहरूका कर्मचारीहरूलाई यसको जेनेरेटिभ एआई च्याटबट प्रयोग गर्न सुरक्षित तरिकाको रूपमा माइक्रोसफ्ट ३६५ कोपाइलट च्याटलाई अगाडि बढाएको छ।

तर हालैको एउटा समस्याका कारण उपकरणले केही उद्यम प्रयोगकर्ताहरूलाई उनीहरूको ड्राफ्टमा भण्डारण गरिएका सन्देशहरू र पठाइएका इमेल फोल्डरहरूबाट जानकारी बाहिर निकालेको बताएको छ - जसमा गोप्य रूपमा चिन्ह लगाइएकाहरू पनि समावेश छन्।

माइक्रोसफ्टले यो समस्या समाधान गर्न एउटा अपडेट ल्याएको र "कसैलाई पनि त्यस्तो जानकारीमा पहुँच प्रदान नगरेको बताएको छ जुन उनीहरूलाई पहिले नै हेर्नको लागि अधिकृत गरिएको थिएन"।

यद्यपि, केही विज्ञहरूले कम्पनीहरूले नयाँ एआई सुविधाहरू थप्न प्रतिस्पर्धा गर्ने गतिले यस्ता गल्तीहरू अपरिहार्य भएको चेतावनी दिएका छन्।

कोपाइलट च्याटलाई आउटलुक र टिम्स जस्ता माइक्रोसफ्ट प्रोग्रामहरू भित्र प्रयोग गर्न सकिन्छ, जुन इमेल र च्याट प्रकार्यहरूको लागि प्रयोग गरिन्छ, प्रश्नहरूको उत्तर प्राप्त गर्न वा सन्देशहरूको संक्षेप गर्न।

"हामीले एउटा समस्या पहिचान गर्यौं र सम्बोधन गर्यौं जहाँ माइक्रोसफ्ट ३६५ कोपाइलट च्याटले प्रयोगकर्ताद्वारा लेखिएका गोप्य लेबल गरिएका इमेलहरूबाट सामग्री फिर्ता गर्न सक्छ र आउटलुक डेस्कटपमा उनीहरूको ड्राफ्ट र पठाइएका वस्तुहरू भित्र भण्डारण गर्न सक्छ," माइक्रोसफ्टका प्रवक्ताले बीबीसी न्यूजलाई भने।

"हाम्रा पहुँच नियन्त्रणहरू र डेटा सुरक्षा नीतिहरू अक्षुण्ण रहे पनि, यो व्यवहारले हाम्रो अभिप्रेत कोपाइलट अनुभव पूरा गरेन, जुन कोपाइलट पहुँचबाट सुरक्षित सामग्रीलाई बहिष्कार गर्न डिजाइन गरिएको हो," तिनीहरूले थपे।

"उद्यम ग्राहकहरूको लागि विश्वव्यापी रूपमा कन्फिगरेसन अपडेट तैनाथ गरिएको छ।"

यो गल्तीको बारेमा पहिलो पटक टेक समाचार आउटलेट ब्लीपिङ कम्प्युटरले रिपोर्ट गरेको थियो , जसले समस्या पुष्टि गर्ने सेवा अलर्ट देखेको बताएको थियो।

यसले माइक्रोसफ्टको सूचनालाई उद्धृत गर्दै भनेको छ कि "गोप्य लेबल लगाइएका प्रयोगकर्ताहरूको इमेल सन्देशहरू माइक्रोसफ्ट ३६५ कोपाइलट च्याटद्वारा गलत तरिकाले प्रशोधन गरिँदैछ"।

सूचनामा थपिएको छ कि कोपाइलट च्याट भित्रको कार्य ट्याबले प्रयोगकर्ताको ड्राफ्ट र पठाइएका फोल्डरहरूमा भण्डारण गरिएका इमेल सन्देशहरूलाई संक्षेपमा प्रस्तुत गरेको थियो, जबकि तिनीहरूसँग संवेदनशीलता लेबल र अनधिकृत डेटा साझेदारी रोक्नको लागि कन्फिगर गरिएको डेटा हानि रोकथाम नीति थियो।

रिपोर्टहरूले सुझाव दिन्छ कि माइक्रोसफ्टलाई जनवरीमा पहिलो पटक त्रुटिको बारेमा थाहा भएको थियो।

बगको बारेमा यसको सूचना इङ्गल्याण्डका NHS कामदारहरूको लागि समर्थन ड्यासबोर्डमा पनि साझा गरिएको थियो - जहाँ मूल कारण "कोड समस्या" लाई जिम्मेवार ठहराइएको छ।

NHS IT समर्थन साइटमा रहेको सूचनाको एक खण्डले यो प्रभावित भएको संकेत गर्छ।

तर यसले बीबीसी न्यूजलाई भनेको छ कि कोपाइलट च्याटद्वारा प्रशोधन गरिएका कुनै पनि मस्यौदा वा पठाइएका इमेलहरूको सामग्री तिनीहरूका सिर्जनाकर्ताहरूसँग रहनेछ, र बिरामीको जानकारी खुलासा गरिएको छैन।

'डेटा चुहावट हुनेछ'

माइक्रोसफ्ट ३६५ कोपाइलट च्याट जस्ता इन्टरप्राइज एआई उपकरणहरू - जुन माइक्रोसफ्ट ३६५ सदस्यता भएका संस्थाहरूका लागि उपलब्ध छन् - मा संवेदनशील कर्पोरेट जानकारीको साझेदारीलाई रोक्नको लागि प्रायः कडा नियन्त्रण र सुरक्षा सुरक्षाहरू हुन्छन्।

तर केही विज्ञहरूका लागि, यो मुद्दाले अझै पनि निश्चित कार्य वातावरणमा जेनेरेटिभ एआई उपकरणहरू अपनाउने जोखिमहरूलाई हाइलाइट गर्दछ।

गार्टनरका डेटा सुरक्षा र एआई शासन विश्लेषक नादेर हेनेनले भने, "नयाँ र नयाँ एआई क्षमताहरू" जारी हुने आवृत्तिलाई ध्यानमा राख्दै, "यस प्रकारको गडबडी अपरिहार्य छ"।

उनले बीबीसी समाचार संस्थाहरूलाई भने कि यी एआई उत्पादनहरू प्रयोग गर्नेहरूमा प्रायः आफूलाई सुरक्षित राख्न र प्रत्येक नयाँ सुविधा व्यवस्थापन गर्न आवश्यक उपकरणहरूको अभाव हुन्छ।

"सामान्य परिस्थितिमा, संस्थाहरूले यो सुविधा बन्द गर्थे र शासन सुदृढ नभएसम्म पर्खन्थे," हेनेनले भने।

"दुर्भाग्यवश, अप्रमाणित एआई प्रचारको धारले निम्त्याएको दबाबको मात्राले यसलाई लगभग असम्भव बनाउँछ," उनले थपे।

सरे विश्वविद्यालयका साइबर-सुरक्षा विज्ञ प्रोफेसर एलन वुडवर्डले भने कि यसले यस्ता उपकरणहरूलाई पूर्वनिर्धारित रूपमा निजी बनाउने र अप्ट-इन मात्र गर्ने महत्त्व देखाएको छ।

"यी उपकरणहरूमा अनिवार्य रूपमा बगहरू हुनेछन्, विशेष गरी जब तिनीहरू तीव्र गतिमा अगाडि बढ्छन्, त्यसैले डेटा चुहावट जानाजानी नभए पनि यो हुनेछ," उनले बीबीसी न्यूजलाई भने।