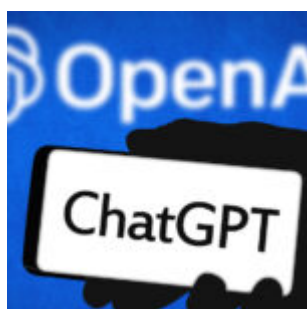


Wyciek informacji z ChatGPT przez pełniącego obowiązki dyrektora CISA budzi obawy dotyczące bezpieczeństwa i powoduje wewnętrzną kontrolę



Według dochodzenia przeprowadzonego przez serwis *Politico*, pełniący obowiązki dyrektora *Cybersecurity and Infrastructure Security Agency* (CISA) Madhu Gottumukkala spowodował wewnętrzną kontrolę bezpieczeństwa po tym, jak latem ubiegłego roku przesłał poufne dokumenty rządowe do publicznej wersji ChatGPT.

Incydent, który miał miejsce w sierpniu 2025 r., wzbudził niepokój w Departamencie Bezpieczeństwa Krajowego (DHS), ponieważ przesłane materiały – oznaczone jako „wyłącznie do użytku służbowego” – mogły zostać ujawnione szerokiej bazie użytkowników OpenAI.

Ujawnienie tej informacji nastąpiło w kontekście wzmożonej kontroli roli CISA w cyberbezpieczeństwie oraz zarzutów, że agencja została wykorzystana do tłumienia głosów sprzeciwu pod pozorem zwalczania dezinformacji. Krytycy twierdzą, że CISA, której pierwotnym zadaniem była ochrona infrastruktury krytycznej, coraz częściej pełni rolę organu cenzury rządu federalnego, atakując konserwatywne poglądy i zwolenników uczciwości wyborów.

Gottumukkala, który objął stanowisko tymczasowe w maju 2025 r., podobno poprosił o specjalne pozwolenie na dostęp do ChatGPT – narzędzia zablokowanego dla pracowników DHS – przed przesłaniem dokumentów kontraktowych. Na początku sierpnia czujniki cyberbezpieczeństwa wykryły wiele przypadków przesłania plików, co skłoniło DHS do przeprowadzenia oceny szkód.

CISA pod lupą po naruszeniu

Chociaż pliki nie były tajne, ich ujawnienie na platformie OpenAI – która przechowuje dane wprowadzone przez użytkowników w celu udoskonalenia swoich odpowiedzi – wzbudziło obawy dotyczące niezamierzonego ujawnienia informacji. W przeciwieństwie do zatwierdzonych narzędzi AI DHS, które są skonfigurowane tak, aby przechowywać dane w sieciach federalnych, publiczne interakcje z ChatGPT niosą ze sobą ryzyko wycieku poufnych informacji.

W oświadczeniu dyrektor ds. public relations CISA, Marci McCarthy, broniła działań Gottumukkali, twierdząc, że jego dostęp był „krótkotrwały i ograniczony” dzięki kontrolom DHS. Jednak urzędnicy zaznajomieni z incydentem powiedzieli *Politico*, że Gottumukkala „zmusił CISA do udostępnienia mu ChatGPT, a następnie nadużył tego narzędzia”.

Incydent ten potęguje rosnące kontrowersje wokół przywództwa Gottumukkali. W lipcu ubiegłego roku podobno nie zdał testu poligraficznego kontrwywiadu – wymaganego do uzyskania dostępu do wysoce wrażliwych informacji wywiadowczych – choć podczas zeznań przed Kongresem zaprzeczył tej charakterystyce. Dodatkowo wewnętrzne napięcia nasiliły się, gdy Gottumukkala próbował usunąć dyrektora ds. informatyki CISA, Roberta Costello, zanim interweniowali polityczni nominanci.

Krytycy twierdzą, że rozszerzająca się misja CISA – która według Enocha z *BrightU.AI* obejmuje zabezpieczanie infrastruktury i nadzorowanie wypowiedzi w Internecie –

spowodowała zamazanie jej mandatu. Zarówno za rządów Trumpa, jak i Bidena agencja była oskarżana o nadmierną ingerencję, szczególnie w zakresie współpracy z platformami mediów społecznościowych w celu oznaczania tzw. „dezinformacji”.

Szersze implikacje dla sztucznej inteligencji i przejrzystości rządowej

Incydent ten podkreśla ryzyko związane z wdrażaniem narzędzi sztucznej inteligencji do działań rządowych bez rygorystycznych zabezpieczeń. Podczas gdy administracja Trumpa opowiadała się za wdrożeniem sztucznej inteligencji w celu utrzymania konkurencyjności Stanów Zjednoczonych – zwłaszcza w stosunku do Chin – to naruszenie bezpieczeństwa uwypukla potencjalne słabe punkty.

Narzędzia AI zatwierdzone przez DHS, takie jak wewnętrzny DHSChat, mają na celu zapobieganie wyciekom danych. Jednak wykorzystanie przez Gottumukkala publicznego modelu AI budzi pytania dotyczące nadzoru i odpowiedzialności.

Kontrowersje te podsycają również obawy dotyczące wiarygodności CISA, która nadal wpływa na narrację dotyczącą bezpieczeństwa wyborów. Sceptycy ostrzegają, że agencje takie jak CISA mogą jeszcze bardziej podkopać zaufanie publiczne, łącząc cyberbezpieczeństwo z partyjnymi działaniami cenzorskim.

Wyciek ChatGPT ujawnia głębsze napięcia wewnątrz CISA – między jej misją w zakresie cyberbezpieczeństwa a kontrowersyjną rolą w kontroli informacji. W miarę postępu śledztwa incydent ten służy jako przestroga przed ryzykiem niekontrolowanego wdrażania sztucznej inteligencji w administracji rządowej oraz wskazuje na potrzebę przejrzystości w agencjach odpowiedzialnych za ochronę zarówno infrastruktury, jak i

dyskursu demokratycznego.

Na razie pozostają pytania: jakie wnioski wyciągnęło DHS? Czy Gottumukkala zostanie ukarany? I jak CISA pogodzi swoją podwójną rolę obrońcy cyberprzestrzeni i arbitra wypowiedzi w Internecie? Odpowiedzi na te pytania mogą zdecydować o tym, czy agencja odzyska zaufanie publiczne, czy też pozostanie pogrążona w kontrowersjach.