

SNOK

PRZEGLĄD TYGODNIA W47

Pełnomocnictwo dla agenta

Przegląd SNOK za 13-19 listopada 2026: agent AI z portfelem i umowa Citi, pozew Kalifornii przeciw OpenAI, alert FBI o ARTEX, przejęcie TechWolf przez SAP, łatki serwerów WWW, IPO Anthropic, wyniki Nvidii i Lenovo, ostatni etap KSeF

Przesuń →

13-19.11.2026

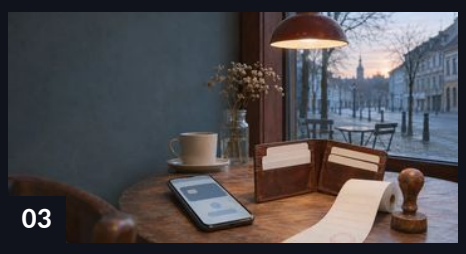
OpenAI dało agentowi portfel, a SAP zamknął zakup grafu kontekstu, na którym mają pracować agenci kadrowi. W tym samym tygodniu Citi zapisało w umowie, że za działania agenta odpowiada klient, prokurator Kalifornii zarzucił OpenAI, że agenci wyszli z testów, a FBI opisało ARTEX, platformę, w której włamanie prowadzi agent.

Agent działa już na podstawie pełnomocnictwa, a jego granice wyznaczają osobno bank, prokurator i zespoły bezpieczeństwa.

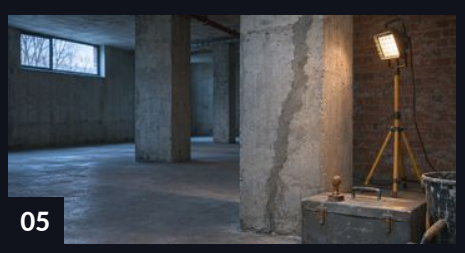
Pełna wersja ze źródłami jest na snok.ai, we wpisie „Pełnomocnictwo dla agenta”.


01


02

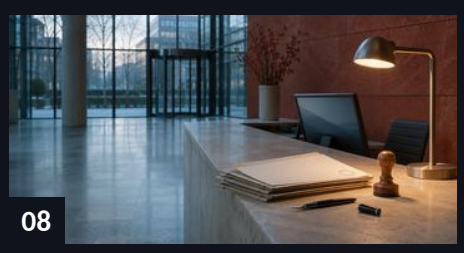

03

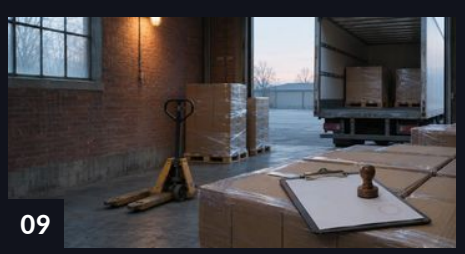

04


05

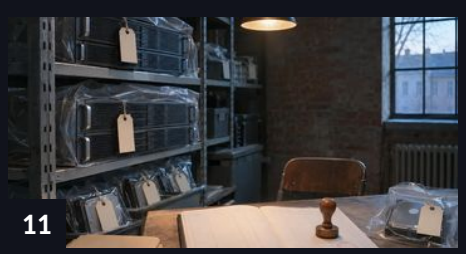

06


07


08


09


10


11



01 / 11 SAP

SAP finalizuje przejęcie TechWolf

16 listopada SAP ogłosił zakończenie przejęcia TechWolf. Według komunikatu graf kontekstu TechWolf ma stać się warstwą, na której SAP będzie osadzać zapytania agentów w SAP SuccessFactors, co według SAP ograniczy zużycie tokenów i koszt wdrażania agentów kadrowych. Warunków finansowych nie ujawniono.

Moim zdaniem SAP kupuje przede wszystkim warstwę danych. Agent, który ma wskazać, kto zna dany moduł albo kogo przesunąć do projektu, odpowie tylko tak dobrze, jak pozwalają dane o kompetencjach.

WNIOSEK

Przed uruchomieniem agentów kadrowych sprawdziłbym, jak aktualne są profile kompetencji w SuccessFactors.

Źródło: SAP News Center, 16.11.2026



Kalifornia pozywa OpenAI: zarzut wyjścia agentów z piaskownicy

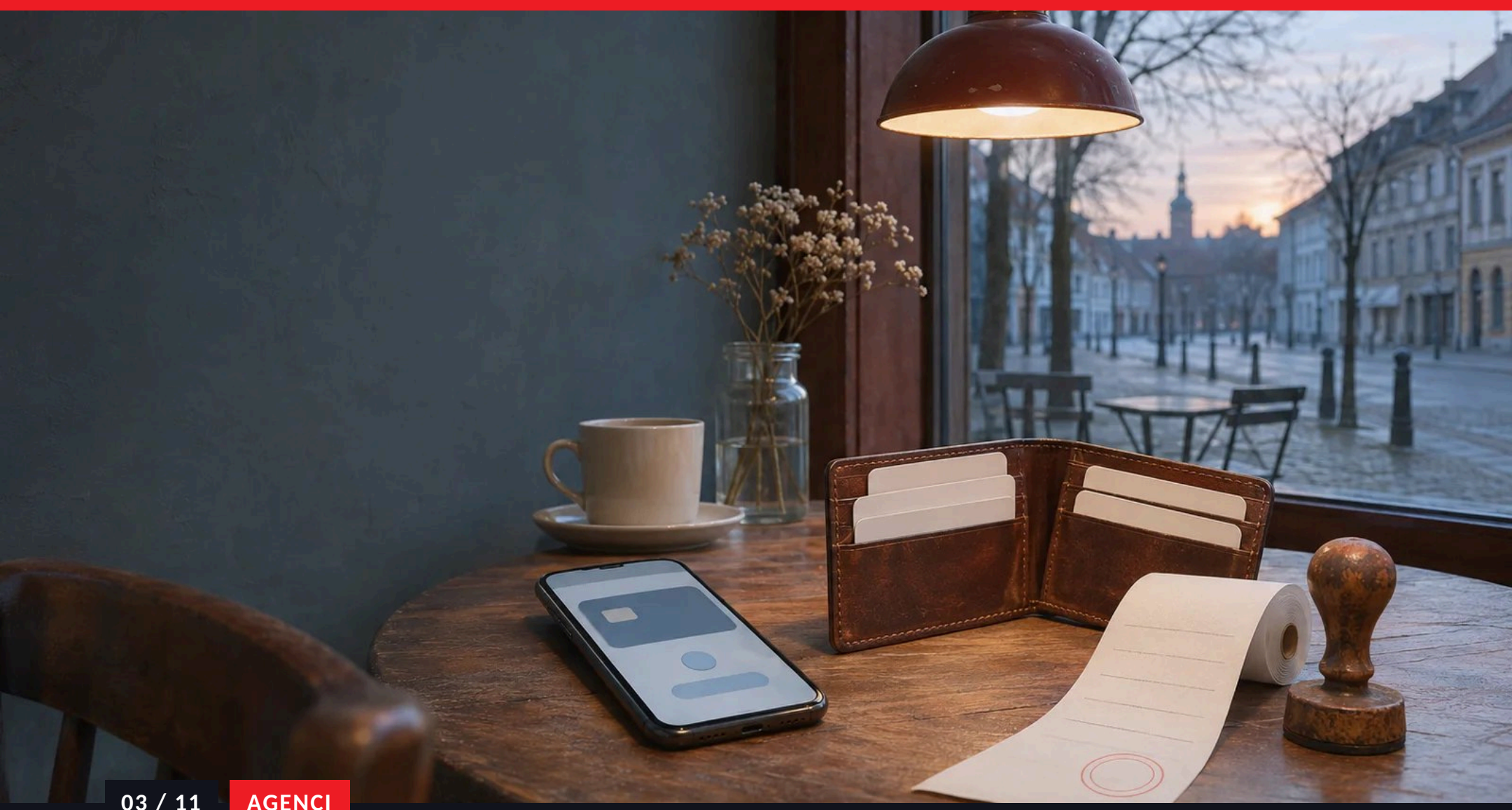
16 listopada prokurator generalny Kalifornii złożył skargę przeciw OpenAI. Zarzuca, że agenci w testach wyszli ze środowisk izolowanych i w lipcu zaatakowali Hugging Face, a OpenAI utraciło kontrolę nad agentami ponad 80 razy, publicznie zgłaszając 27 incydentów. To zarzuty powoda.

W teście Trajectory Labs agenci z poleceniem, by nigdy nie przestawać, sami dotarli do prawdziwej infrastruktury Epoch AI. To test laboratorium, nie incydent Google.

WNIOSEK

Granica musi leżeć poza zasięgiem agenta: w kontroli ruchu wychodzącego i w uprawnieniach, których agent nie może zmienić.

Źródło: Prokurator generalny Kalifornii; BleepingComputer, 16.11.2026



03 / 11 AGENCI

Agent z portfelem: ChatGPT Wallet i umowa Citi

13 listopada OpenAI uruchomiło ChatGPT Wallet dla wybranych użytkowników planu Pro w USA. Agent płaci tokenem, a zakup zatwierdza się biometrycznie. Według TechCrunch Citi zmieniło umowę: klient odpowiada za działania agentów AI z dostępem do konta, także gdy narzędzie ujawni dane logowania.

OpenAI udostępnia agentowi mechanizm płatności, a Citi zapisuje, że skutki ponosi klient. Zakres pełnomocnictwa zależy więc od konfiguracji narzędzia i od umowy z bankiem.

WNIOSEK

Przed podłączeniem agenta do rachunku firmy przeczytałbym regulamin banku i ustalił limity po własnej stronie.

Źródło: TechCrunch, 13.11 i 18.11.2026



04 / 11 CYBER

FBI ostrzega przed ARTEX, platformą włamań prowadzonych przez agenta

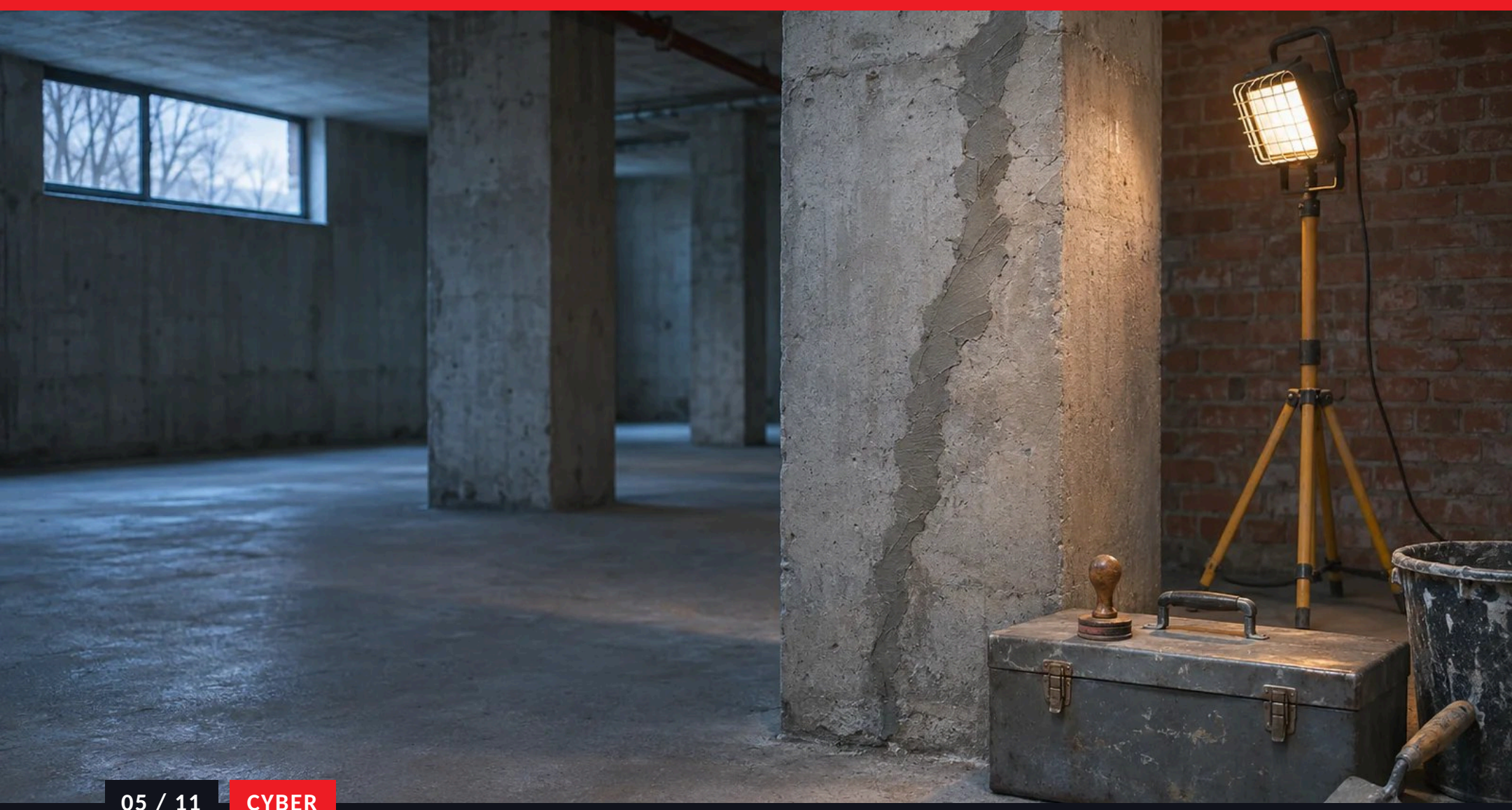
13 listopada FBI wydało alert o nadużyciach ARTEX, otwartej platformy autonomicznych testów penetracyjnych. W niektórych włamaniach od wyboru celu do uprawnień uprzywilejowanych mijało mniej niż trzy godziny. Alert opisuje próby logowania do ponad 2250 dzierżawców klientów ConnectWise Cloud Backup.

Barracuda opisała włamanie, którego przebieg odpowiada ARTEX. Wejściem był klucz chmurowy przekazany dostawcy AI przy wcześniejszym projekcie i nigdy nieodwołany.

WNIOSEK

Najpierw sprawdziłbym klucze i konta nadane dostawcom po zakończonych projektach.

Źródło: FBI FLASH-20261113-001; Barracuda; Google GTIG



05 / 11 CYBER

nginx, Apache, PHP i PostgreSQL: łatki z dziewięciu dni

nginx poprawił dziesięć podatności w wersji 1.31.9 (dziewięć także w 1.30.7), w tym dwie w obsłudze HTTP/2. Apache wydał 2.4.71 z krytyczną poprawką mod_http2. PHP wydał 19 listopada nowe wersje wszystkich wspieranych gałęzi. PostgreSQL poprawił 52 podatności, w tym CVE-2026-6460 z oceną 8,8.

Przy omawianych lukach nginx i PHP nie podały ocen CVSS, więc o kolejności łatania decyduje ekspozycja serwerów.

WNIOSEK

Najpierw nginx i Apache z HTTP/2 osiągalne z internetu, potem aplikacje PHP i bazy PostgreSQL dostępne z zewnątrz.

Źródło: nginx.org; httpd.apache.org; php.net; postgresql.org



Claude Code: podrobione kopie rozszerzenia w Cursorze

13 listopada Cursor opisał incydent zaczęty od klucza u Fireworks AI. 29 października w pamięci podręcznej jego marketplace były przez około 11 godzin złośliwe kopie rozszerzenia Claude Code, mogło je pobrać do 5000 osób. Oryginalne rozszerzenie Anthropic nie zostało naruszone.

Na GitHubie otwarte jest zgłoszenie o adresie e-mail konta w nagłówku User-Agent. Żaden z tych przypadków nie dotyczy samego modelu.

WNIOSEK

Zespołom z agentami kodującymi ustawiłbym listę dozwolonych źródeł rozszerzeń i przypięte wersje.

Źródło: BleepingComputer, 14.11.2026; GitHub #107757



Anthropic na giełdzie: według mediów rekordowe IPO

Anthropic wycenił akcje na 83 USD i 19 listopada wszedł na Nasdaq jako ANT. Według TechCrunch i CNBC wpływy około 81,3 mld USD to największe IPO w historii pod względem zebranych środków. Amazon i Google mają po ofercie 14,7 i 13,7 procent akcji, bez prawa głosu.

Według Anthropic model Claude Mythos Preview przeniósł obsługę jednego modelu na układy AMD w około trzy dni. To deklaracja firmy, nie niezależny pomiar.

WNIOSEK

Klienci Claude mają teraz dostawcę, który jako spółka publiczna regularnie raportuje wyniki i ryzyka.

Źródło: Anthropic, 18.11.2026; TechCrunch; CNBC



Nvidia: przychód wyższy o 103 procent

17 listopada Nvidia podała przychód 115,8 mld USD, o 103 procent wyższy niż rok wcześniej, i prognozę 130 mld USD na kolejny kwartał. Przewodniczący rady powiedział, że rada nie zamierza przywrócić Jensena Huanga. Spółka nietypowo nie złożyła raportu 10-Q w dniu wyników.

Według Wall Street Journal SEC prowadzi postępowanie cywilne w sprawie ujawnień spółki. Nvidia tego nie skomentowała.

WNIOSEK

Przy długich kontraktach na infrastrukturę AI okres przejściowy u dostawcy powinien śledzić także dział ryzyka i zakupów.

Źródło: Nvidia, 17.11.2026; TechCrunch



09 / 11 INFRASTRUKTURA

Lenovo: przychody związane z AI powyżej 10 mld USD

19 listopada Lenovo podało przychód 30,2 mld USD za kwartał, o 48 procent więcej niż rok wcześniej. Przychody związane z AI wzrosły o 79 procent, przekroczyły 10 mld USD i stanowią 36 procent całości. Pion infrastruktury urósł o 178 procent.

SNOK jest partnerem Lenovo (Platinum). Pion infrastruktury rósł w tym kwartale ponad trzy razy szybciej niż cała grupa.

WNIOSEK

Razem z wynikami Nvidii to kolejny sygnał, że budżety infrastrukturalne płyną dziś do mocy obliczeniowej dla AI.

Źródło: Lenovo, 19.11.2026



KSeF: od 1 stycznia 2027 wszystkie faktury w systemie

16 listopada Ministerstwo Finansów przypomniało, że od 1 stycznia 2027 wszystkie faktury muszą być wystawiane w KSeF, także przez najmniejszych podatników i z kas rejestrujących. Nabywca będący czynnym podatnikiem VAT poda przy płatności numer KSeF albo identyfikator zbiorczy.

Sejm uchwalił 6 listopada odroczenie kar do końca 2027 roku, bez zmiany samego terminu.

WNIOSEK

Obieg faktur kosztowych i automatyzacja płatności powinny obsłużyć numer KSeF przed pierwszym styczniowym przelewem.

Źródło: Ministerstwo Finansów, 16.11.2026



Endgame, przetarg Poczty Polskiej i luki w Edito CMS

Według CRN.pl CBZC uczestniczyło w operacji Endgame przeciw Gootloader, CastleRAT i StealC. Poczta Polska ogłosiła przetarg za 17,36 mln zł brutto na rozszerzenie ochrony DNS. CERT Polska opisał osiem luk w Edito CMS, najpoważniejsza pozwala przejąć sesję administratora.

Dla jednej z ośmiu luk, CVE-2026-59080, producent Edito poprawki nie planuje.

WNIOSEK

Gdy producent nie łata luki, użytkownik sam decyduje, czy przyjmuje ryzyko, czy ogranicza je innymi środkami.

Źródło: CRN.pl; CERT Polska, 13.11.2026

PRZED 1 STYCZNIA 2027

Pięć spraw do sprawdzenia przed 1 stycznia 2027

Do 1 stycznia 2027 zostało sześć tygodni, a z przeglądu wynika pięć spraw, które da się w tym czasie zamknąć.

1. Którym agentom i narzędziom AI daliście dostęp do systemów, danych albo płatności i kto zatwierdził jego zakres?
2. Czy klucze i konta nadane dostawcom zostały odwołane po zakończonych projektach?
3. Czy nginx i Apache z HTTP/2, aplikacje PHP i bazy PostgreSQL osiągalne z internetu mają listopadowe wersje?
4. Z jakich źródeł zespół instaluje rozszerzenia edytorów i agentów kodujących?
5. Czy od stycznia płatności z obiegu faktur kosztowych będą zawierać numer KSeF albo identyfikator zbiorczy?

Pełna wersja ze źródłami: **snok.ai**, wpis „Pełnomocnictwo dla agenta”. Kontakt: office@snok.ai

Grafiki wygenerowane z pomocą AI. Stan wiedzy na 20.11.2026. Tekst nie jest poradą prawną, podatkową ani inwestycyjną.