Informacja Prasowa

Czas na systemowe podejście – ALEET o bezpieczeństwie danych operacyjnych w logistyce i transporcie w erze AI

(Warszawa, 24.04.2026) - Dynamiczna cyfryzacja branży logistyczno-transportowej oraz rosnące wykorzystanie AI w zarządzaniu procesami i flotami sprawiają, że dane operacyjne to najcenniejsze zasoby organizacji, a ich ochrona staje się coraz większym wyzwaniem. Eksperci ALEET, twórcy bliźniaka cyfrowego floty, zwracają uwagę, iż skuteczna ochrona danych nie jest już wyłącznie domeną działów IT, lecz wymaga skoordynowanego podejścia obejmującego całą organizację, od operacji po zarządzanie strategiczne. Wnioski te znajdują potwierdzenie w raporcie ISACA State of Cybersecurity 2025.

Niedofinansowanie i luka kompetencyjna

Z raportu ISACA (Information Systems Audit and Control Association) wynika, że 55% zespołów cyberbezpieczeństwa jest niedofinansowanych, a 65% organizacji zmaga się z nieobsadzonymi stanowiskami w obszarze bezpieczeństwa. Jednocześnie tylko 29% firm inwestowało w ubiegłych latach w przekwalifikowanie pracowników do ról bezpieczeństwa (spadek z 41% w roku 2024), mimo że 70% ekspertów tego obszaru przewiduje dalszy wzrost zapotrzebowania na specjalistów. W sektorze logistyczno-transportowym, gdzie systemy operacyjne są ściśle powiązane z danymi w czasie rzeczywistym, oznacza to realne wyzwania dla ciągłości działania.

- W ALEET traktujemy bezpieczeństwo danych operacyjnych jako element strategiczny, który musi być wbudowany w architekturę systemu od samego początku. Nasze bliźniaki cyfrowe flot do zarządzania transportem projektujemy tak, aby ochrona danych, kontrola dostępu i ciągłe monitorowanie zagrożeń były integralną częścią środowiska operacyjnego, a nie warstwą dodaną na późniejszym etapie. Dzięki temu organizacje korzystające z naszych technologii budują realną odporność, opartą nie tylko na narzędziach, ale na spójnym, bezpiecznym modelu zarządzania danymi w całej organizacji – mówi dr Katarzyna Marczuk, Prezeska Zarządu ALEET.

Kto powoduje zagrożenie – technologia czy człowiek?

Raport ISACA wskazuje, że główne wektory cyberataków to inżynieria społeczna (44%), wykorzystanie podatności (37%) oraz złośliwe oprogramowania (26%). Jednocześnie 43% specjalistów ds. cyberbezpieczeństwa uważa atak za bardzo prawdopodobny w ciągu najbliższego roku. W środowisku logistycznym, gdzie dane operacyjne są rozproszone i wykorzystywane w wielu punktach organizacji, zagrożenia te mają charakter systemowy.

- Największą zmianą, jaką obserwujemy, jest przesunięcie punktu ciężkości z pojedynczych incydentów na zarządzanie całym ekosystemem danych. Dzisiaj, cyberataki nie dotyczą już jednego systemu, mogą wpływać na ciągłość operacji, łańcuchy dostaw i relacje z partnerami. Organizacje potrzebują nie tylko narzędzi, ale spójnej strategii bezpieczeństwa, która obejmuje ludzi, procesy i technologie – wskazuje przedstawicielka ALEET.

Systemowy problem

Z raportu wynika również, że 66% specjalistów ds. cyberbezpieczeństwa odczuwa większy stres niż pięć lat temu, a 47% odejść z pracy wynika bezpośrednio z jego wysokiego poziomu. To efekt kumulacji czynników takich jak niedobory kadrowe, rosnąca liczba zagrożeń oraz presja operacyjna. ISACA wskazuje na deficyty w zakresie kompetencji miękkich to jest myślenia krytycznego (57%), komunikacji (56%) i rozwiązywania problemów (47%).

- Bezpieczeństwo danych operacyjnych wymaga dziś zdolności do podejmowania decyzji w warunkach niepewności oraz efektywnej współpracy między działami. To obszar, w którym technologia musi być wspierana przez kompetencje organizacyjne. Tutaj istotne jest budowanie kultury bezpieczeństwa obejmującej wszystkich pracowników, nie tylko specjalistów IT. Widzimy wyraźnie, że organizacje, które polegają wyłącznie na zespołach IT, dochodzą do granicy wydolności. Dlatego coraz większego znaczenia nabiera współpraca z wyspecjalizowanymi partnerami technologicznymi. Pozwala ona nie tylko odciążyć zespoły wewnętrzne, ale przede wszystkim wprowadzić standardy bezpieczeństwa już na etapie projektowania systemów – zauważa dr Katarzyna Marczuk.

AI wspiera bezpieczeństwo – pod warunkiem właściwego wdrożenia

Zgodnie z ISACA, 47% organizacji pracuje nad AI governance, a 40% wdraża rozwiązania oparte na sztucznej inteligencji. Najczęstsze zastosowania obejmują wykrywanie zagrożeń (32%), bezpieczeństwo punktów końcowych (30%) oraz automatyzację zadań (28%).

- AI staje się naturalnym elementem systemów operacyjnych w logistyce, ale jego rola w bezpieczeństwie zależy od jakości implementacji. W ALEET traktujemy AI jako narzędzie wspierające analizę i predykcję zagrożeń w środowisku operacyjnym. Kluczowe jest jednak to, że AI działa w ramach kontrolowanej architektury, w której bezpieczeństwo danych jest założeniem projektowym, a nie dodatkiem. Nasze bliźniaki cyfrowe flot umożliwiają nie tylko przetwarzanie danych, ale także pełną kontrolę nad ich przepływem, wykrywanie anomalii w czasie rzeczywistym oraz symulowanie scenariuszy zagrożeń. Dzięki temu organizacje zyskują nie tylko efektywność, ale również realną odporność na ryzyka – podkreśla dr Katarzyna Marczuk, Prezeska Zarządu ALEET.

Wnioski płynące z raportu ISACA są jednoznaczne - bezpieczeństwo danych nie może być ograniczone do jednej funkcji czy działu IT w organizacji. W środowisku opartym na AI konieczne jest podejście całościowe, obejmujące wszystkie poziomy działalności. Oznacza to integrację bezpieczeństwa z procesami operacyjnymi, inwestycję w kompetencje oraz współpracę z partnerami, którzy posiadają doświadczenie w budowaniu bezpiecznych środowisk danych. W branży logistyczno-transportowej jest to warunek utrzymania ciągłości operacyjnej i przewagi konkurencyjnej.

***

Kontakt dla prasy:
contact@aleet.co