**Kontakt dla mediów:**

Patrycja Kaleta-Łuczynowicz

patrycja.kaleta@linkleaders.pl

+48 505 223 994

Olga Skarżyńska

olga.skarzynska@linkleaders.pl

M: +48 510 382 420

**Połowa polskich firm uznaje zależność od producentów oprogramowania spoza Polski i Europy za zagrożenie [najnowszy raport ESET]**

**Europa przyspiesza budowanie odporności – militarnej, gospodarczej i cyfrowej. Wojna w Ukrainie, rosnące napięcia w relacjach globalnych oraz oznaki niepewności po stronie Stanów Zjednoczonych sprawiają, że unijne państwa coraz mocniej stawiają na własne zasoby i technologie. Polska znajduje się w tej układance w szczególnie trudnym położeniu – w pierwszej połowie 2025 roku była krajem z największą liczbą wykrytych ataków ransomware na świecie. Nic więc dziwnego, że krajowe firmy coraz wyraźniej dostrzegają wagę cyfrowej suwerenności. Jak pokazuje najnowszy raport** [***Cyberportret polskiego biznesu 2025***](https://in.eset.pl/cyberportret-polskiego-biznesu)**opublikowany przez ESET i DAGMA Bezpieczeństwo IT, 49% polskich firm wskazuje, że zależność od producentów oprogramowania spoza Polski i Europy może stanowić zagrożenie, a 57% przy wyborze oprogramowania ds. cyberbezpieczeństwa bierze dziś pod uwagę kraj pochodzenia producenta. Suwerenność cyfrowa to nie tylko polityczne hasło, lecz wymierny element strategicznego bezpieczeństwa.**

**Najważniejsze dane:**

* 49% ekspertów ds. cyberbezpieczeństwa wskazuje, że zależność od producentów spoza Polski i Europy może stanowić zagrożenie dla firmy.
* 59% przedsiębiorstw preferuje rozwiązania od producentów z Europy
* 67% badanych ekspertów zwraca uwagę na lokalizację centrów danych.
* połowa firm w Polsce zauważa wzrost liczby ataków
* Polska jest najczęściej atakowana ransomware na świecie

Przez dekady Europa budowała swoją cyfrową infrastrukturę, w dużej mierze opierając się na partnerach zza oceanu. Taki model wydawał się naturalny, a globalne rozwiązania były gwarantem stabilności i źródłem najważniejszych technologii. Dziś jednak ten paradygmat się zmienia. W miarę jak rośnie rywalizacja globalna, a napięcia polityczne przenikają do sfery gospodarki i technologii, Europa coraz częściej musi stawać na własnych nogach.

Nie chodzi już tylko o konkurencyjność rynkową, ale o strategiczne bezpieczeństwo. W obliczu wojny w Ukrainie i rosnących zagrożeń hybrydowych, od ataków cybernetycznych po manipulację łańcuchami dostaw, uzależnienie od jednego źródła technologii staje się ryzykowne. Tym bardziej że również po stronie Stanów Zjednoczonych pojawiają się oznaki niestabilności. Plany cięć budżetowych w amerykańskiej Agencji Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) na 2026 rok[[1]](#footnote-1) wywołały dyskusję, czy Europa może pozwolić sobie na dalsze poleganie wyłącznie na wsparciu partnera transatlantyckiego.

W tym kontekście koncepcja suwerenności cyfrowej przestaje być akademickim pojęciem, a staje się realną strategią. To właśnie ona ma umożliwić państwom unijnym budowanie odporności na wstrząsy geopolityczne i unikanie strategicznych słabości.

 - Krajobraz geopolityczny staje się coraz bardziej złożony, a porządek światowy, jaki znaliśmy przez dekady, ulega zasadniczym zmianom. Długoletnie relacje z kluczowymi partnerami są coraz częściej wystawiane na próbę. W tej nowej rzeczywistości Europa i unijni decydenci coraz mocniej akcentują potrzebę większej samodzielności regionu – zarówno poprzez wykorzystywanie własnych atutów, jak i eliminowanie strategicznych słabości, aby nie pozostawać w tyle za innymi globalnymi graczami, czy to w zakresie rozwoju europejskiej infrastruktury cyfrowej, czy zdolności obronnych – mówi **Andy Garth, Director of Government Affairs, ESET**.

**Strategiczne wybory zamiast prostych kalkulacji**

Zmiana podejścia nie jest teorią, lecz praktyką widoczną w decyzjach biznesowych. Coraz więcej polskich firm świadomie wybiera technologie z Europy, traktując je jako bezpieczniejsze i bardziej przewidywalne. Dane z najnowszego raportu *Cyberportret polskiego biznesu 2025* pokazują, że 59% przedsiębiorstw preferuje rozwiązania pochodzące z naszego kontynentu.To nie tylko gest lojalności wobec europejskich marek, ale przede wszystkim element strategii opartej na zgodności z unijnymi regulacjami i standardami ochrony danych.

Niepokój o stabilność globalnych łańcuchów dostaw widać także w postrzeganiu ryzyka. Połowa ekspertów odpowiadających za cyberbezpieczeństwo wskazuje, że zależność od producentów spoza Polski i Europy może stanowić zagrożenie dla ich organizacji. Firmy zaczynają więc kalkulować nie tylko cenę i funkcjonalność rozwiązań, lecz także potencjalne konsekwencje geopolityczne związane z wyborem technologii. Z pewnością wpływ mają na to coraz bardziej złożone relacje UE z Azją i Stanami Zjednoczonymi.

Co istotne, ta ostrożność narasta. 69% specjalistów IT przyznaje, że w ostatnich latach zwiększyło czujność wobec pochodzenia producentów rozwiązań, a 66% wiąże tę zmianę bezpośrednio z wydarzeniami globalnymi – od pandemii, przez wojnę w Ukrainie, po napięcia w relacjach między największymi mocarstwami. To oznacza, że świadomość biznesu w Polsce staje się coraz bardziej dojrzała i odporna na uproszczone kalkulacje.

**Im większy biznes, tym większa waga cyfrowej suwerenności**

Dane z raportu jasno pokazują, że 67% specjalistów w Polsce zwraca uwagę na lokalizację centrów danych. To sygnał, że fizyczne umiejscowienie infrastruktury przestaje być kwestią techniczną, a staje się jednym z podstawowych kryteriów wyboru technologii.

Warto zważyć, że widoczne są wyraźne różnice w podejściu do suwerenności cyfrowej w zależności od wielkości firmy. W dużych organizacjach odsetek ten sięga 71%, podczas gdy w średnich – 62%. Dane wskazują więc jasno: im większa firma, tym więcej uwagi poświęca kwestii cyfrowej suwerenności.

- Dane pokazują, że polskie firmy coraz uważniej podchodzą do kwestii pochodzenia technologii. W dużych organizacjach świadomość ta jest najwyższa, ale generalnie widać, że temat cyfrowej suwerenności mocno zyskał na znaczeniu w całym biznesie. To bardzo ważne, bo Polska jest dziś jednym z krajów szczególnie narażonych na cyberataki. W takim otoczeniu decyzje oparte na bezpieczeństwie i przewidywalności partnerów mają kluczowe znaczenie - mówi **Paweł Jurek, Dyrektor działu rozwoju biznesu w DAGMA Bezpieczeństwo IT**.

**Polska szczególnie narażona na cyberataki**

Polska znalazła się w pierwszej połowie 2025 roku na pierwszym miejscu na świecie pod względem liczby wykrytych ataków ransomware. To jasno pokazuje, że nasz kraj należy dziś do najbardziej narażonych na działania cyberprzestępców. Firmy potwierdzają tę eskalację: 48% firm zauważa wzrost liczby ataków, a 46% – rosnącą różnorodność metod stosowanych przez przestępców.

Widać też mocny ruch wśród rosyjskich grup cyberprzestępczych. To, co dzieje się w Ukrainie, stanowi ważną lekcję dla Polski: klasyczne działania zbrojne są ściśle powiązane z aktywnością w cyberprzestrzeni. Przykładem jest działalność grup Turla i Gamaredon, które współpracują jeszcze od czasów zimnej wojny, a dziś prowadzą zaawansowane operacje cyberszpiegowskie.

Ostatnie półrocze pokazało, że cyberprzestrzeń coraz wyraźniej staje się elementem globalnych napięć. Najbardziej aktywne grupy APT pochodzą z Chin (ponad 40% ataków), Rosji (25,7%), Korei Północnej (14,4%) i Iranu (9,1%)[[2]](#footnote-2). Ich aktywność pokrywa się z wydarzeniami geopolitycznymi – tam, gdzie narastają konflikty i napięcia, rośnie też intensywność ataków. To potwierdza, że cyberbezpieczeństwo nie może być traktowane w oderwaniu od szerszego kontekstu geopolitycznego.

Doświadczenia ostatnich miesięcy pokazują, że polski biznes potrafi wyciągać wnioski z otoczenia geopolitycznego. Świadomość znaczenia cyfrowej suwerenności jest dziś wyraźnie widoczna w firmach i to właśnie ona staje się jednym z kluczowych elementów odporności w warunkach rosnącej presji cyberataków.

- Europa dysponuje ogromnym potencjałem ludzkim i eksperckim. To właśnie w Unii Europejskiej powstały firmy, które osiągnęły pozycję liderów rynkowych w takich obszarach jak łączność cyfrowa czy e-zdrowie. Obecna niepewność geopolityczna oraz nasilająca się globalna konkurencja gospodarcza stanowią jednocześnie ostrzeżenie i szansę na wzmocnienie europejskiego przemysłu oraz przyspieszenie rozwoju technologii kluczowych dla przyszłego dobrobytu regionu – podsumowuje **Andy Garth**.

**O raporcie**

„[Cyberportret polskiego biznesu 2025](https://in.eset.pl/cyberportret-polskiego-biznesu)”, przygotowany przez ESET i DAGMA Bezpieczeństwo IT, przedstawia aktualny obraz cyberbezpieczeństwa w polskich firmach. To kontynuacja badania zapoczątkowanego w 2024 roku, które ma na celu uchwycenie zmian w podejściu polskich przedsiębiorstw do zagrożeń cyfrowych, a także oceny ich gotowości na coraz bardziej złożone wyzwania technologiczne i geopolityczne. Raport zestawia ze sobą perspektywy pracowników i osób odpowiedzialnych za cyberbezpieczeństwo firm.

Z danych wynika, że przedsiębiorstwa mierzą się z coraz bardziej złożonymi zagrożeniami, a luka między deklarowaną wiedzą a realnymi działaniami wciąż jest niepokojąco szeroka. Autorzy raportu analizują nie tylko skalę ataków i poziom zabezpieczeń, ale także świadomość pracowników, skuteczność szkoleń i gotowość organizacji do wdrażania nowych standardów w dynamicznie zmieniającej się rzeczywistości.

Badanie zostało zrealizowane w dniach od 23 czerwca do 8 lipca 2025 roku przez ARC Rynek i Opinia na próbie liczącej łącznie 1040 Polaków pracujących przy komputerze co najmniej 3 dni w tygodniu, w tym 283 osoby zaangażowane w obszar cyberbezpieczeństwa w firmach zatrudniających co najmniej 10 pracowników. Próba objęła również „boost” w wysokości N=251 ekspertów ds. IT. Zastosowano technikę ankiety online (CAWI)

1. <https://www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts> [↑](#footnote-ref-1)
2. ESET APT Activity Report Q4 2024–Q1 2025 [↑](#footnote-ref-2)