***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* *agnieszka.juraszczyk@capgemini.com*

***Kontakt dla prasy:***

*Olga Skarżyńska*

*+48 510 382 420*

*E-mail:* olga.skarzynska@linkleaders.pl

**Dlaczego firmy muszą szyfrować dane… z myślą o komputerach, których jeszcze nie ma? Postkwantowa kryptografia wchodzi do gry**

**Wielkimi krokami zbliża się era komputerów kwantowych – a wraz z nią nowe zagrożenia dla bezpieczeństwa danych. Choć technologia ta wciąż się rozwija, firmy już dziś powinny przygotować się na moment, gdy dotychczasowe metody szyfrowania przestaną działać. Nowy raport Capgemini nie pozostawia złudzeń: ponad połowa organizacji na świecie uważa, że „Q-Day”, czyli przełom, który pozwoli łamać obecne zabezpieczenia, nastąpi w ciągu dekady. Stawką są dane, zaufanie klientów, zgodność z regulacjami i przewaga konkurencyjna.**

**Q-Day: tykająca bomba w świecie danych**

Q-Day, czyli moment, gdy komputery kwantowe złamią dzisiejsze standardy szyfrowania, przestaje być futurystyczną wizją. 61% firm z grupy Early Adopters (tych, które już działają w zakresie PQC lub planują działania wkrótce) uważa, że nastąpi to w ciągu dziesięciu lat.

Zagrożenie jest realne. Obecne algorytmy RSA i ECC mogą nie sprostać przyszłej mocy obliczeniowej. Co więcej – dane można przechwycić już dziś i odszyfrować za kilka lat („harvest now, decrypt later”). Obawia się tego 65% organizacji. Na szali leżą m.in. dane klientów, dokumentacja medyczna, własność intelektualna.

– Pojawienie się pełnoskalowych, odpornych na błędy komputerów kwantowowych, jakie są prezentowane na roadmapach największych graczy na rynku, może podzielić świat organizacji na te, które były gotowe, i te, które będą gasić pożar – ostrzega **Marek Kowalik, Quantum Software Developer w Capgemini Polska** – To nie tylko upgrade. To zmiana paradygmatu.

57% firm nie czeka – już wdraża zasady postkwantowej kryptografii, niezależnie od tempa rozwoju nowych maszyn.

**Start już był. Niektórzy są na ostatnim okrążeniu**

Postkwantowa kryptografia przestaje być niszowym tematem. Dla liderów to konkretne harmonogramy i partnerstwa technologiczne. Kluczowe sektory nie tylko reagują – inicjują zmianę.

W branży obronnej 90% organizacji planuje wdrożenie quantum-safe rozwiązań w ciągu pięciu lat. W bankowości – 86%, w lotnictwie – 83%. Dla porównania: w sektorze FMCG czy handlu detalicznym to tylko 48–49%.

70% firm uznaje PQC za nieodzowny element strategii bezpieczeństwa. Tyle samo wskazuje je jako najskuteczniejszą odpowiedź na zagrożenia kwantowe. 62% przewiduje, że w nadchodzących latach postkwantowe podejście stanie się standardem.

– Jeszcze niedawno miernikiem dojrzałości była adopcja chmury. Dziś jest nią odporność kryptograficzna – komentuje **Marek Kowalik, Quantum Software Developer w Capgemini Polska** – Firmy, które inwestują w PQC, pokazują gotowość na wyzwania kolejnej dekady.

**Kto zostaje w tyle, ten ryzykuje więcej, niż myśli**

W takich branżach jak handel, FMCG, transport czy hotelarstwo poziom przygotowania do PQC jest niski. 56% organizacji to dopiero „beginners”, a tylko 15% ma solidne fundamenty – zarówno techniczne, jak i organizacyjne.

To już nie tylko luka technologiczna. To także ryzyko wizerunkowe. Klienci pytają o zabezpieczenia danych, a regulatorzy przygotowują nowe obowiązki. Opóźnienia mogą oznaczać nie tylko utratę danych, ale i zaufania – zasobu dziś trudniejszego do odbudowania niż dostęp do budżetu IT.

**Nie brakuje woli, brakuje ludzi. I strategii**

Firmy dostrzegają zagrożenie, ale 67% wskazuje na brak budżetów i zasobów. Tymczasem pierwsze kroki – jak audyt kluczy, inwentaryzacja algorytmów czy mapowanie zależności – nie wymagają jeszcze nowej infrastruktury.

Wśród barier: brak ekspertów (59%), przestarzałe systemy (54%) i problemy z kompatybilnością rozwiązań. Przejście na PQC bywa organizacyjnie trudne, ale ten proces sam się nie skróci. Lepiej zacząć teraz, niż nadrabiać w pośpiechu.

**Zwlekasz? Możesz nie zdążyć**

30% firm nie planuje wdrożeń PQC w najbliższych pięciu latach. 65% nie uznaje zagrożenia za pilne. 67% czeka na standardy (np. NIST). 68% – na budżet.

Jednocześnie 70% tej grupy przyznaje, że wzrost cyberzagrożeń i nowe regulacje mogą wymusić gwałtowne działania. Tyle że wtedy może być za późno. PQC to nie „łatka”, a transformacja – z testami, harmonogramami, edukacją. Na to potrzeba lat – nie tygodni.

Jak pokazuje raport Capgemini, różnicę między liderami a resztą wyznacza dziś czas reakcji. Wygrywają ci, którzy już mapują systemy szyfrowania, edukują zespoły i włączają odporność kryptograficzną do strategii bezpieczeństwa – z poziomu zarządu.

– To nie wyścig zbrojeń, tylko wyścig o zaufanie – podsumowuje **Marek Kowalik, Quantum Software Developer w Capgemini Polska** – Wygrają ci, którzy zbudują odporne środowisko cyfrowe, zanim komputery kwantowe rozbroją te słabe. A zdążą tylko ci, którzy działają zwinnie – bo crypto-agility to nowy standard dojrzałości. Pytanie nie brzmi: czy jesteśmy gotowi? Tylko: czy zdążymy.

**O Capgemini**

Capgemini jako globalny partner w zakresie transformacji biznesowej i technologicznej, pomaga organizacjom przyspieszyć ich transformację w kierunku cyfrowego i zrównoważonego świata, jednocześnie wywierając realny wpływ na biznes i społeczeństwo. Capgemini jest odpowiedzialną i wielokulturową firmą, liczącą 350 000 osób zatrudnionych w ponad 50 krajach. Dzięki silnemu 55- letniemu dziedzictwu cieszy się zaufaniem swoich klientów, wykorzystując moc technologii i w pełni zaspokajając ich potrzeby biznesowe. Dostarcza kompleksowe usługi i rozwiązania, oparte o swoje najmocniejsze strony: od strategii i projektowania rozwiązań po inżynierię, jakie są napędzane przez wiodące na rynku technologie z zakresu sztucznej inteligencji, generatywnej sztucznej inteligencji, chmury i danych, połączone z szeroką wiedzą branżową i siecią partnerów. W 2024 roku Grupa odnotowała globalne przychody w wysokości 22,1 miliardów euro.

Get The Future You Want | [www.capgemini.com](http://www.capgemini.com#_blank)