***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* [*agnieszka.juraszczyk@capgemini.com*](mailto:agnieszka.juraszczyk@capgemini.com)

***Kontakt dla prasy:***

*Olga Skarżyńska*

*+48 510 382 420*

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

**Czy zmiany w Kodeksie Pracy wpłyną na bezpieczeństwo pracy hybrydowej i zdalnej?**

**Już 7 kwietnia 2023 roku zaczną obowiązywać nowe regulacje Kodeksu Pracy dotyczące pracy zdalnej i hybrydowej. Ten model zatrudnienia wprowadziło na stale aż 89%[[1]](#footnote-1) firm. Jednym z największych wyzwań związanych z pracą poza siedzibą organizacji jest bezpieczeństwo danych. Czy zmiany prawne wpłyną na jego poprawę?**

Praca zdalna stanowi wyzwanie nie tylko z punktu widzenia kultury organizacyjnej firmy. W sytuacji, gdy ludzie wykonują swoje obowiązki spoza biura, używając do tego prywatnego sprzętu, pojawiają się też inne dodatkowe problemy. W modelu pracy stacjonarnej, niemalże każda firma zatrudniała dedykowany zespół IT, którego zadaniem było dbanie o zabezpieczenia sieci korporacyjnej. Praca z domu generuje nowe ryzyka i niebezpieczeństwa czyhające na zatrudnione osoby, które w większości nie mają specjalistycznej wiedzy w zakresie cyberbezpieczeństwa.

- Zmiany w Kodeksie Pracy, które niebawem zaczną obowiązywać, nakładają na pracodawcę obowiązek zapewnienia każdej osobie zatrudnionej w trybie hybrydowym lub zdalnym niezbędnych do wykonywania pracy narzędzi technicznych. Oddzielając w ten sposób sferę zawodową od prywatnej, zmniejszamy ryzyko, że osoby pracujące w naszej firmie staną się ofiarami np. phishingu i dojdzie do wycieku zarówno prywatnych, jak i firmowych danych – mówi **Grzegorz Borowiec, Head of Security Community we wrocławskim oddziale Capgemini Polska** i dodaje -Samo zapewnienie firmowego sprzętu nie zagwarantuje jednak znacznej poprawy bezpieczeństwa. Dodatkowo potrzeba wdrożyć procesy zapewniające m.in. szyfrowanie dysków twardych i pamięci przenośnych na wypadek fizycznej utraty np. kradzieży lub zgubienia. Tego rodzaju zabezpieczenia są standardem w Capgemini Polska. Nasi eksperci z działu testów starają się nie tylko przewidywać potencjalne zagrożenia, ale też aktywnie im przeciwdziałać.

- W Capgemini wdrożyliśmy szereg zabezpieczeń fizycznych, elektronicznych i organizacyjnych, które mają na celu kompleksową ochronę sprzętu i aplikacji służących do pracy zdalnej. Bezpieczne połączenie z naszą siecią online w trakcie pracy zdalnej zapewnia stosowanie VPN. Wykorzystujemy też inne rozwiązania, na przykład szyfrowanie danych, oprogramowanie antywirusowe, firewalle – dodaje **Marta Maciejuk-Cierpiszewska, Information Security Officer z wrocławskiego oddziału Capgemini Polska.**

Bardzo ważnym zagadnieniem jest również edukacja pracowników. Osoby zajmujące się na co dzień zadaniami z dziedzin niezwiązanych bezpośrednio z cyberbezpieczeństwem, powinny posiadać przynajmniej podstawową wiedzę na temat zagrożeń i sposóbów ochrony.

- Wiedza z zakresu cyberbezpieczeństwa to w obecnych czasach podstawa. W Capgemini stale przypominamy pracownikom o najważniejszych zasadach, czyli ustawianiu (i regularnym zmienianiu) silnych i unikalnych haseł wszędzie, także w domowych sieciach Wi-Fi, nieużywaniu sieci publicznych, blokowaniu komputerów i przede wszystkim nieprzesyłaniu firmowych dokumentów na prywatne maile lub za pomocą komunikatorów. Zwracamy też dużą uwagę na fizyczne bezpieczeństwo naszej infrastruktury, co potwierdzone jest wieloma certyfikatami. Regularne szkolenia z bezpieczeństwa informacji są u nas obowiązkowe dla każdego pracownika – komentuje **Michał Mikucki, Dyrektor poznańskiego oddziału Capgemini Polska**.

Dodatkowym aspektem całkowitego odejścia od sztywnego modelu pracy biurowej w przeważającej liczbie firm, jest większe zainteresowanie technologią chmury, która poza tym, że w oczywisty sposób ułatwia pracę zdalną, znacząco wpływa również na poprawę bezpieczeństwa danych. Systemy chmurowe wyposażone są w najnowsze i stale rozwijane systemy zabezpieczeń. Dodatkowo przechowywanie danych w chmurze może pomóc zmniejszyć ryzyko zagrożeń związanych z błędami popełnianymi przez osoby pracujące. Dzięki tej technologii jesteśmy w stanie prawie całkowicie wyeliminować m.in. przechowywanie danych firmowych na urządzeniach typu pendrive, które mogą być nośnikami złośliwego oprogramowania oraz przesyłanie materiałów na prywatne adresy e-mail.

Praca zdalna oraz hybrydowa jest i będzie codziennością w większości firm. Możemy być pewni, że jej popularność w najbliższych latach nie będzie spadać. W obecnych czasach, kiedy pozyskiwanie talentów stanowi wyzwanie, a konkurencja pomiędzy pracodawcami jest silna, coraz większym priorytetem staje się utrzymanie osób pracujących na dłużej - jak pokazują badania naukowców z Uniwersytetu Stanforda, w firmach które wprowadziły na stałe model pracy hybrydowej rotacja pracowników spadła aż o 1/3[[2]](#footnote-2). Aby jednak ten model pracy był bezpieczny zarówno dla firm, jak i dla ich klientów, konieczne jest utrzymywanie najwyższych możliwych standardów cyberbezpieczeństwa. Nowe regulacje prawne z pewnością wesprą takie działania, jednak nie zastąpią profesjonalnego przygotowania po stronie pracodawców.

**O Capgemini**

Capgemini to światowy lider w dziedzinie doradztwa w zakresie transformacji i zarządzania biznesem poprzez wykorzystanie mocy technologii. Celem Grupy jest dążenie do odpowiedzialnej społecznie, zintegrowanej i zrównoważonej przyszłości, w której potencjał ludzki jest wspierany nowymi technologiami. Capgemini jest odpowiedzialną i wielokulturową organizacją, liczącą ponad 360 000 pracowników zatrudnionych w ponad 50 krajach. Dzięki silnemu 55-letniemu dziedzictwu i szerokiej wiedzy branżowej cieszy się zaufaniem swoich klientów, a także jest zdolna kompleksowo zaspokoić ich potrzeby biznesowe: od strategii i projektowania rozwiązań po działania operacyjne napędzane przez dynamicznie rozwijający się i innowacyjny świat technologii chmury, danych, sztucznej inteligencji, łączności, oprogramowania, inżynierii cyfrowej i platform. W 2022 roku Grupa odnotowała globalne przychody w wysokości 22 miliardów euro.

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

1. Raport „Hybrid and Beyond” przygotowany przez Colliers we współpracy z HRK i serwisem Well.hr [↑](#footnote-ref-1)
2. Badanie Uniwersytetu Stanforda rozpowszechnione przez National Bureau of Economic Research [↑](#footnote-ref-2)