

Praca zdalna dla wielu Polaków stała się codziennością za sprawą wybuchu pandemii COVID-19. Ostatnio doczekała się ona nawet uregulowania w kodeksie pracy. Taka forma wykonywania obowiązków zawodowych ma istotny wpływ na ochronę przetwarzanych danych w firmach, urzędach i instytucjach. Pracodawcy wraz z pracownikami wykonującymi pracę zdalną muszą więc zapewnić odpowiedni poziom bezpieczeństwa danych – najczęściej poprzez wdrożenie właściwych procedur i systematyczne szkolenia.

Nowelizacja Kodeksu Pracy, którą w styczniu br. podpisał prezydent, wprowadziła możliwość wykonywania pracy częściowo lub całkowicie w miejscu wskazanym przez pracownika każdorazowo uzgodnionym z pracodawcą lub na jego polecenie. Na pracodawców zostały nałożone obowiązki zapewnienia pracownikowi:

- materiałów do wykonywania pracy zdalnej,
- instalacji, serwisu, konserwacji narzędzi do pracy lub pokrycie kosztów z tym związanych,
- szkoleń i pomocy technicznej niezbędnej do wykonywania pracy.

Praca zdalna a ochrona danych

Jedną z najbardziej istotnych regulacji dotyczących pracy zdalnej są obowiązki odnoszące się do ochrony danych osobowych zawarte w art. 67 KP. Dotyczą one zasad tworzenia przez firmy odpowiednich procedur ochrony danych oraz instrukcji postępowania i szkoleń w tym zakresie. Budując taki system ochrony danych, można skorzystać ze wskazówek zawartych w normach serii ISO/IEC 27000.

Jak wskazuje ekspert ds. cyberbezpieczeństwa DEKRA - Przygotowując procedury bezpieczeństwa, trzeba uwzględnić zagrożenia, jakie pojawiają się w trakcie wykonywania pracy zdalnej np. kradzież telefonu czy laptopa, zainfekowanie szkodliwym oprogramowaniem, użycie niechronionych sieci bezprzewodowych. Nie wolno też zapominać o zagrożeniach pojawiających się w fizycznym miejscu świadczenia pracy zdalnej, choćby możliwość podejrzenia przez osoby trzecie informacji na monitorze. Identyfikacja potencjalnych zagrożeń pozwala opracować właściwą politykę bezpieczeństwa.

Tworząc założenia takiej polityki, należy zwrócić uwagę na następujące kwestie dotyczące bezpieczeństwa przetwarzanych danych:

- zasady bezpiecznej komunikacji, w tym dostępu do systemów organizacji przy wykorzystaniu mechanizmów uwierzytelniania. Warto uwzględnić również słabości jednoczynnikowych mechanizmów uwierzytelniania i rozważyć wprowadzenie dwuczynnikowego uwierzytelniania (2FA),
- zasady zabezpieczenia przed nieuprawnionym dostępem do informacji lub zasobów ze strony osób trzecich (rodzina czy znajomi) przebywających w miejscu pracy zdalnej,
- zasady zabezpieczenia przed nieuprawnionym dostępem osób trzecich w miejscach publicznych oraz bezpiecznego wykorzystania sieci domowych i publicznych, w tym wymogi dotyczące takich sieci,
- zasady konfiguracji urządzeń w przypadku pracy poza siedzibą organizacji,
- zasady użycia urządzeń prywatnych do wykonywania obowiązków służbowych.

Pracownicy muszą być świadomi zagrożeń

(Cyber)bezpieczna praca zdalna wyzwaniem dla pracodawcy

Kategoria: Aktualności

Opublikowano: środa, 01, marzec 2023 12:16

Katarzyna Sekuła

Odsłony: 725

Jednak samo stworzenie procedur nie okaże się wystarczającym zabezpieczeniem dla przetwarzanych danych, jeśli pracownicy nie będą ich znali i przestrzegali. Trzeba pamiętać, że cyberprzestępcy wykorzystują coraz to nowsze metody, by wejść w posiadanie wrażliwych danych.

Źródło: IP