Wysyłanie PIT-a drogą mailową

Wstęp

Niniejszy artykuł ma na celu rozwiać wątpliwości dotyczące kwestii wysyłania PIT-a drogą elektroniczną. Należy tutaj zaznaczyć, iż nie dotyczy to tylko kwestii poczty elektronicznej ale również ogólnodostępnych narzędzi, które między innymi służą do udostępniania konkretnych plików / dokumentów konkretnemu gronu odbiorców. Nie można tutaj oczywiście mówić tylko o kwestii konkretnego dokumentu jakim jest PIT, lecz najważniejszą kwestią jest katalog danych osobowych jaki jest przesyłany.

Zabezpieczanie dokumentu hasłem

Na samym początku należy zaznaczyć, iż za pomocą służbowej poczty mamy możliwość wysyłania plików. Pracodawca daje nam taką możliwość w celu wykonywania przez pracowników powierzonych im zadań. Wielu pracodawców posiada wewnętrzne procedury dotyczące kwestii przesyłania maili. Mowa tutaj o automatycznym przekierowywaniu maili, ustawianiu autorespondera oraz kwestii wymogu szyfrowania plików, które zawierają dane osobowe. Należy pamiętać, iż katalog danych osobowych nie jest katalogiem zamkniętym i niejednokrotnie procedury te nie posiadają wymienionych konkretnych danych osobowych lecz jedynie określenie, iż plik który posiada dane osobowe (wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej) powinien być zabezpieczony hasłem. Jak widać, jeśli posiadamy wątpliwości czy dane zawarte w pliku mogą zawierać się w definicji danych osobowych, to bezpieczniej będzie po prostu ten plik zaszyfrować.
Pojawia się tutaj kolejna wątpliwość odnośnie formy przekazania hasła. Czy można tutaj wykorzystać ten sam kanał, którym to został przekazany zaszyfrowany plik? Niestety kanał przekazania hasła dostępu do pliku powinien być inny niż ten, który przekazał zaszyfrowane dane. Najlepiej jest podać telefonicznie hasło osobie, do której był kierowany dokument albo przesłanie go sms. Wszelkie te działania mają na celu zmniejszenia ryzyka dostępu osób postronnych do danych zawartych w zaszyfrowanych plikach. Wysłanie hasła tym samym kanałem, co zaszyfrowane pliki pozwala w przypadku przełamania zabezpieczeń tego kanału do bezproblemowego dostępu do zaszyfrowanych danych, w tym danych osobowych.

Mail jako kanał przekazania PIT

Powyżej zostało przedstawiona najlepsza forma zapewniania przekazania pliku z danymi osobowymi. Należy zaznaczyć, że w PIT posiadamy wszelkie informacje, które pozwalają zidentyfikować osobę, do której PIT należy. W tym szczególnym przypadku należy podjąć wszelkie możliwe kroki, w celu zapewnienia nie tylko bezpieczeństwo ale także integralność danych osobowych zawartych w dokumencie. W celu zapewnienia integralności przekazywanych danych należy pamiętać, by przekazywany plik był w formacie PDF oraz był on opatrzony elektronicznym podpisem kwalifikowanym. Dzięki przyjęciu takiego formatu wraz z zastosowaniem podpisu kwalifikowanego mamy pewność, iż dane zawarte w dokumencie to te które powinny być oraz, kto podpisał dokument. Dodatkowo mamy

pewność, iż wartości zawarte w dokumencie nie zostały zmienione, gdyż jakakolwiek ingerencja w dokumencie usuwa podpis kwalifikowany.
Kwestie przekazania mamy już opisaną. Pojawia się kwestia tego, czy PIT powinien zostać przesłany na adres służbowy czy też prywatny. O ile nie ma problemu co do przesyłania PIT obecnemu pracownikowi, to pojawia się wątpliwość jak należy przesłać PIT do pracownika, który już nie pracuje, a co za tym idzie nie korzysta z poczty służbowej. W mojej ocenie nie ma problemu wykorzystać do tego celu maila prywatnego, który został podany przez pracownika. Należy jednak tutaj pamiętać, by pracodawca był w stanie wykazać, iż faktycznie przekazał PIT pracownikowi. Należy tutaj przyjąć, iż pracodawca do byłego pracownika powinien zadzwonić w celu przekazania hasła oraz zweryfikowania czy nadal wykorzystuje maila oraz otrzymał PIT.

Podsumowanie
Jak zostało to przedstawione w niniejszym artykule, to nie ma przeciwskazań by przesyłać PIT w wersji elektronicznej drogą mailową. Należy przy tym pamiętać o zasadach, zgodnie z którymi trzeba dokonać wysyłki oraz zapewnić poufność danych osobowych, które są przesyłane.

Mateusz Jakubik – specjalista ds. ochrony informacji w iSecure Sp. z o.o.