aut. Sylwia Gliwa 23.05.2019

PODPIS ELEKTRONICZNY - ŁATWY I WYGODNY, ALE CZY BEZPIECZNY? [WYWIAD]

Wykorzystanie podpisu elektronicznego to nie tylko wygoda i oszczędność czasu. Pozwala on również na zachowanie pełnej kontroli nad łańcuchem przepływu dokumentów, co z kolei przekłada się na możliwość ograniczenia ryzyka związanego z zachowaniem poufności danych. Jednak czy wykorzystanie podpisu jest tak samo bezpieczne jak własnoręczny podpis? Jakie korzyści ma zastąpienie tradycyjnego obiegu dokumentów w firmie? O tym jak uniknąć niepotrzebnego ryzyka związanego z wykorzystaniem podpisu elektronicznego oraz jakie są newralgiczne elementy systemu mówi ekspert DocuSign, Piotr Mroziński.

Podpis elektroniczny jest coraz popularniejszy zarówno w dużych korporacjach jak i w sektorze małych i średnich przedsiębiorstw, jako narzędzie mające skrócić czas obiegu dokumentów. Czy za uproszeniem pracy idzie również poprawa bezpieczeństwa?

Spójrzmy na karty płatnicze. Kiedyś mówiło się, że karta płatnicza czy kredytowa musi mieć ustawiony limit i koniecznie musi być podpisana, aby zweryfikować tożsamość z dowodem osobistym. Potem nabraliśmy większego poczucia bezpieczeństwa przy ich użytkowaniu i stwierdziliśmy, że w zupełności wystarczy PIN - w sumie działa tak samo, a nie ma potrzeby się legitymować. Dzięki temu człowiek nie czuje się jak na przesłuchaniu, a również jest to bezpieczne. Teraz są już transakcje dotykowe i nawet karty nie trzeba wyciągać z portfela tylko płacimy telefonem i dalej jest rozwiązanie bezpieczne.

Podpis elektroniczny sam w sobie jest bezpieczny, tak samo jak karta kredytowa, którą wykorzystujemy do płacenia. Kiedy mówimy o bezpieczeństwie w podpisie elektronicznym to mylimy dwie rzeczy: to jaka jest tożsamość tego użytkownika i jaka jest waga potwierdzenia jego tożsamości i upewnienia się, że ten podpis opowiada podpisowi ręcznemu, a jaka jest potrzeba, aby ten podpis był zrobiony łatwo, szybko i bezpiecznie dla wszystkich. Ważne, aby podpis elektroniczny dał ten sam efekt co ręczny a pozwolił zminimalizować cały proces, czas czy papier.

Krótki przegląd poradników czy ofert firm oferujących te rozwiązania na rynku posługują się 3 terminami: podpis elektroniczny, bezpieczny podpis elektroniczny i kwalifikowany podpis elektroniczny. Zacznijmy od podstaw – czym te rodzaje podpisów różnią się od siebie?

Poprzez bezpieczny podpis elektroniczny, w Polsce definiuje się po prostu podpis kwalifikowany. Na zachodzie nie mówimy o bezpiecznym podpisie elektronicznym, bo każdy musi być bezpieczny. Jak spojrzysz sobie na infrastrukturę dowolnego systemu podpisu elektronicznego to jest ona zupełnie taka sama. Dokument, który przepływa jest tak samo zabezpieczony i wygląda identycznie. Jedynym elementem, który się różni jest element potwierdzania tożsamości i podpisu kwalifikowanego. Jest to pewnego typu miskoncepcja terminologii – bo zamiast mówić o bezpiecznym, powinniśmy mówić o podpisie kwalifikowanym, bo każdy podpis jest bezpieczny. Do 80% transakcji wystarczy nam zwykły podpis elektroniczny. W sensie technologicznym wyróżniamy jego trzy poziomy.

Pierwszy to jest podpis standardowy. Najczęściej wykorzystywany jest do podpisywania NDA (umowa poufności – przyp. red.) lub innych dokumentów, które są zdefiniowane przez prawo. Od strony technicznej wygląda to tak, że jedna osoba przesyła drugiej dokument do podpisu poprzez maila. Osoba, do której skierowano dokument otwiera maila np. w DocuSign, klika „podpisz" i podpis zostaje złożony. Ten system jest bezpieczny, tak samo jak wspomniane wyżej transakcje dotykowe. Jakość tego podpisu jest przyjazna dla użytkownika, podobnie jak płacenie kartą płatniczą. Użytkownik jest identyfikowany przez określoną liczbę parametrów i ma to moc sprawczą.

Kolejnym jest zaawansowany podpis elektroniczny, który systemowo prawie się nie różni. W kontekście potwierdzania tożsamości występują tam dwa elementy. Jednym z nich jest np. kod SMS, który trzeba wpisać przy podpisaniu. I on jest porównywalny do profilu zaufanego. Czyli mamy dodatkowe potwierdzenie tożsamości – użytkownik oprócz tego, że ma swoją skrzynkę pocztową i ma do niej dostęp, to posiada również telefon komórkowy na który przychodzi potwierdzenie. Czyli istnieją dwa poziomy potwierdzenia i jednocześnie podwójne wyrażenie woli. Użytkownik podpisując dokument elektronicznie wyraża zgodę, że chce go podpisać elektronicznie, a tu w tym wypadku jest jeszcze dodatkowo pytany czy aby na pewno chcesz go podpisać. Tak naprawdę jakby ktoś chciał ukraść i wykorzystać podpis to musiałby shackować konto e-mail oraz np. telefon komórkowy, żeby podpisać dokument i aby to działanie nabrało jakiegoś skutku prawnego.

Ostatnim rodzajem jest podpis kwalifikowany. Różni się tym, że ktoś wcześniej zweryfikował w pełni tożsamość użytkownika. Czyli użytkownik pokazał dowód osobisty, ktoś spojrzał na dokument, potem popatrzył na użytkownika i stwierdził, że ta osoba z dowodu to jest dokładnie ten użytkownik i przypisał do niego kartę z pewnymi atrybutami, która weryfikuje, że to jesteś właśnie ta osoba. Skutek prawny pomiędzy zwykłym podpisem elektronicznym a kwalifikowanym podpisem elektronicznym, jeżeli ustawa pozwala, aby dokument był podpisany podpisem zwykłym jest zupełnie taki sam.

Jeśli skutek prawny jest taki sam do czego służy podpis kwalifikowany i w jakim celu z niego korzystać?

Przy dokumentach, które mają wyższą wagę użytkownik potrzebuje wyższy etap potwierdzania tożsamości. Ustawa jasno definiuje jakiego rodzaju są to dokumenty. Podpis kwalifikowany jest odpowiednikiem podpisu ręcznego. Należy pamiętać, że przy korzystaniu z podpisu w biznesie jak i przy sprawach prywatnych tam, gdzie się dodaje kolejne etapy jest to coraz mniej przyjemne. Jeżeli nie ma takiej wyraźnej potrzeby, nie musimy stosować podpisu kwalifikowanego, aby nie komplikować całego procesu. Z punktu widzenia bezpieczeństwa zarówno w biznesie jak i w życiu prywatnym zabezpieczenia są dokładnie takie same.

Który element w łańcuchu technologicznym przy użytkowaniu elektronicznego podpisu jest najbardziej newralgicznym elementem systemu?

Spójrzmy na system trochę szerzej. My jako dostawcy rozwiązań postrzegamy świat jako system umów. Każda firma ma właśnie taki system umów, nie ważne czy to są umowy o pracę, czy o powierzenie sprzętu, czy może umowy z kontrahentami. Tam, gdzie występuje tradycyjny obieg papierowych dokumentów, przechodzą one przez pewien szereg stopni.

Na początku musza być gdzieś stworzone – wyznaczona osoba w firmie je tworzy, zaciąga dane z różnych systemów, pisze ją w Wordzie i następnie zapisuje w pdf. I już na tym etapie powstaje niebezpieczeństwo, że coś pójdzie niezgodnie z myślą – zrobi się literówkę, przekopiuje się zbyt dużo informacji. I zaraz po tym jak dokument zostanie stworzony idzie on dalej w formie papierowej aż do etapu podpisu. W takim typowym systemie obiegu papierowego, ktoś musi ten dokument wydrukować. I tu zaczynają się problemy i pomyślmy co się dzieje – jeśli drukarka jest dalej niż 5 metrów to dokument może leżeć, potem zapominamy, ten dokument znajduje się pomiędzy innymi

wydrukami. Na tym etapie pojawia się niebezpieczeństwo, że ten dokument może trafić w nieuprawnione ręce. Potem jest on niesiony, zazwyczaj przez asystenta, który kładzie go na biurku właściwej osoby i leży w oczekiwaniu na podpis. Z jednej strony czas jaki jest potrzebny do pozyskania podpisu zaczyna nam się przedłużać, a z drugiej strony jego los jest coraz mniej kontrolowalny. Dochodzimy do etapu, że dokument jest podpisywany, skanowany i przesyłany dalej. I znowu zaczynają się problemy - ktoś zrobi literówkę w mailu i z drukarki zostanie przesłany gdzieś indziej a potem rozesłany zostanie do dwóch stron, przechodzi przez maila, zazwyczaj w formie nieszyfrowanej. I to nie koniec naszych działań, dokument jak został podpisany, to musi wykonać jakieś działania. Najpierw w firmie sprawdzamy czy ten dokument został właściwie wypełniony, czy ktoś postawił parafkę tam, gdzie trzeba, czy gdzieś jej nie zabrakło. Następnie ten dokument i tak po raz kolejny wrzucamy do systemu, aby mógł on dalej wywołać kolejne skutki. A na końcu musi on zostać zarchiwizowany na jakimś serwerze firmy.

Tak właśnie wygląda system offline. Zauważyliśmy, że to nie do końca wpisuje się w rzeczywistość XXI wieku i jak firmy funkcjonują. Stworzyliśmy koncept DocuSign Agreement Cloud, która powoduje to, że na każdym etapie życia dokumentu my jesteśmy wstanie ten proces uprościć, spersonalizować, stworzyć go bardziej efektywnym no i też przede wszystkim bezpieczniejszym. Jeśli w firmie wykorzystuje się program sprzedażowy i pracownik chce, aby dane klienta pojawiły się na zamówieniu – jednym kliknięciem jest wstanie wrzucić to do dokumentu, który już został przygotowany i wypełniony. Przesyła go do podpisu, czy to do podpisu zwykłego, jeśli chce to do podpisu zaawansowanego, a jeśli jest to dokument niezwykłej wagi to do podpisu kwalifikowanego. I znowuż jest to podpisywane w tym samym systemem. Co więcej użytkownik ma pełną widoczność kto ten dokument otworzył. Wszystkie systemy które pojawiły się na przestrzeni ostatnich 20 lat, mają na celu poprawę efektywności pracownika i poprawę efektywności firmy. Mają doprowadzić do tego, że systemy są wstanie zautomatyzować i wykonać dużą część pracy. Dążymy do tego i chcemy osiągnąć dokładnie ten sam efekt w odniesieniu do podpisu elektronicznego. Potem pojawia się również kwestia jak zabezpieczony jest ten dokument, który zostaje przesyłany.

Posiadając ten system, użytkownik ma wgląd i pełną kontrolę nad łańcuchem, w to jakie osoby uczestniczą w procesie i może je zdefiniować. Na końcu po podpisaniu dokumentu, automatycznie może pojawiać się on również w systemach fakturowych i znowu oszczędzamy czas, zmniejszamy koszty i przede wszystkim zwiększamy bezpieczeństwo.

W jakim stopniu bezpieczeństwo stosowania podpisów elektronicznych warunkowane jest poprzez użytkowany sprzęt? Co się stanie, jeżeli podpis elektroniczny używany jest na zainfekowanym sprzęcie?

Sprzęt nie ma tak naprawdę wpływu. Bardziej chodzi o to czy ktoś jest wstanie przejąć kontrolę nad tożsamością użytkownika. Jeżeli ktoś shackuje maila i np. będzie posiadał kopie dowodu osobistego i będzie wstanie podpisać z dowolnego urządzenia, dowolny dokument np. profilem zaufanym. Bardziej chodzi o to czy użytkownik jest wstanie chronić swoją tożsamość niż w jaki sposób chroni swój sprzęt.

Najczęściej napotykane problemy to te wynikające z integracji z innymi systemami. Wtedy coś nie działa i trzeba sprawdzić co nie działa. Zazwyczaj są to błędy popełniane przez człowieka. Wykorzystywanie programów takich jak DocuSign wymaga bardzo krótkiego przeszkolenia dla administratora, czyli dla osoby, która wysyła dokument do podpisu.

Podpis elektroniczny stał się codziennym narzędziem pracy jako znacznie bezpieczniejszy i mniej podatny na fałszerstwa niż własnoręczny podpis. Jakie zasady higieny bezpieczeństwa zalecane są przy realizacji czynności związanych z elektronicznymi podpisami?

Po pierwsze nie wysyłaj dokumentów do podpisu na ogólny adres e-mail, tylko bezpośrednio na imienne maile osób do których ma trafić dokument. Po drugie, i to się tyczy podpisującego - jeżeli nie spodziewasz się dokumentu, nie podpisuj go nawet jak pochodzi z wewnątrz organizacji. Trzecim elementem - spójrz, skąd przychodzi e-mail z prośbą o podpisanie dokumentu, czy to nie jest specjalnie wygenerowany mail do przesłania dokumentu mającego na celu wyłudzenie danych lub środków finansowych.

Coraz częściej firmy zaczynają stosować platformy zaufanej trzeciej strony, aby uniknąć przesyłania danych wrażliwych np. o zmianie numeru bankowego do swoich partnerów biznesowych. Stawiają na pewność, że ten dokument pochodzi bezpośrednio od osoby, która jest do tego upoważniona i nikt w niego nie ingerował.

Na rynku istnieje wiele opcji do wyboru, jeśli chodzi o dostawców podpisu. Na co zwrócić uwagę przy doborze podpisu, jeśli chodzi o komfort i bezpieczeństwo użytkowania? Czy sposób doboru podpisu będzie odmienny dla celów biznesowych i prywatnych?

Jak w każdym systemie trzeba zdefiniować co tak naprawdę jest potrzebne organizacji. Czy potrzeba jest jedynie pozyskać podpis i przesłać dokument od punktu A do punktu B? Czy jest niezbędne, aby dokument coś wykonał po tym jako zostanie podpisany, bo nagle po podpisie masz sztab ludzi, którzy obrabiają dokumenty? Trzeba zdefiniować co firma jest wstanie osiągnąć po wprowadzeniu systemu, a następnie spojrzeć na całe życie dokumentów, czy na całe życie umów jakie są w firmie. Zobaczyć, jak one przepływają i co one wywołują, co można zautomatyzować i uprościć. Jeśli jesteś małym przedsiębiorcą, który potrzebuje jedynie podstawowych funkcjonalności po prostu kieruj się ceną. Jeżeli potrzebujesz systemu do bardziej zaawansowanych działań i do większej automatyzacji, wybierz bardziej rozbudowane narzędzia. Wszystkie te rozwiązania są bezpieczne.