

Możesz mieć dane zaszyfrowane, tylko kto ma klucze?

Bezpieczeństwo danych

Z Przemysławem Kucharzewskim, dyrektorem sprzedaży Cypherdog rozmawialiśmy o poufności i bezpieczeństwie danych, skutkach ich wycieku oraz ich ochronie dzięki rozwiązaniom szyfrowania asymetrycznego i blockchain.

Poznajcie bliżej jedną z firm należących do MAIN Partner Community.

CYPHER.DOG®



Mówi się, że dane to złoto XXI wieku. Co to w praktyce oznacza dla firm?

Dane stanowią podstawę funkcjonowania firm, są najcenniejszym zasobem. Ich utrata może oznaczać przerwanie ciągłości działania, straty wizerunkowe i finansowe. Bez dostępu do danych wiele przedsiębiorstw nie jest w stanie kontynuować produkcji czy świadczenia usług.

Wiąże się to ze spadkiem zaufania klientów, a w niektórych scenariuszach nawet brakiem płynności finansowej. W przypadku wycieku danych osobowych dochodzą również kary administracyjne z tytułu RODO.

Niebezpieczeństwo wystąpienia takich sytuacji rośnie – każdy z nas słyszał o coraz częstszych cyberatakach nie tylko gdzieś na świecie, ale i w Polsce. Dlatego skuteczne zabezpieczenie komunikacji firmowej powinno być jednym z priorytetów w każdej branży.

Większość przedsiębiorstw posiada różne rodzaje zabezpieczeń, a nawet szyfruje część danych.

To prawda, ale w takiej sytuacji zawsze zadaję jedno, istotne pytanie:
"Możesz mieć dane zaszyfrowane, tylko kto ma klucze?"

Przedstawię moją ulubioną analogię. Porównajmy miejsce, w którym trzymamy dane czy naszą pocztę do coraz popularniejszego self-storage. Chcemy się dostać do naszej skrzynki, ale zanim to zrobimy musimy udowodnić recepcjoniście, że faktycznie jesteśmy jej właścicielem. Pokazujemy dowód albo otrzymujemy od recepcjonisty sms potwierdzający, lub podajemy dane osobowe – 4 cyfry peselu i nazwisko panięńskiej matki. Dopiero wtedy otrzymujemy klucz do naszej skrzynki.

Brzmi niby bezpiecznie, ale w rzeczywistości każdy element tej sytuacji jest obciążony ryzykiem. Dowód można podrobić – tzw. dowody kolekcjonerskie chociażby, a dane osobowe można znaleźć w Internecie, wystarczy znać podstawy OSINT-u. W przypadku samego klucza – recepcjonista posiada jego kopię "na wszelki wypadek". Mogą go odwiedzić odpowiednie służby lub ktoś się za nie podszywać. Recepcjonista "nie chcąc mieć problemów" odda nasz "prywatny" klucz.

To tak jakby zainstalować drzwi pancerne, a potem schować klucz pod wycieraczkę.

W takim razie, jak firmy mogą zapewnić sobie pełną poufność i bezpieczeństwo danych?

Mieć swój prywatny klucz w kieszeni. Co to oznacza? Przede wszystkim wybrać rozwiązanie, które jest zdecentralizowane, w stu procentach poufne i bezpieczne. Z takim właśnie zamierzeniem stworzyliśmy Cypherdog – alternatywę dla poczty elektronicznej oraz platform wymiany plików. Zapewniamy użytkownikom bezpieczne przysyłanie plików i wiadomości tekstowych, szyfrowany dysk w chmurze oraz szyfrowanie lokalnych zasobów.

Wykorzystujemy szyfrowanie asymetryczne end-to-end, co oznacza, że w wymianie danych lub wiadomości biorą udział dwa klucze – publiczny, używany do szyfrowania i dostępny dla każdego oraz prywatny – niezbędny do odszyfrowania. Niestety, w przypadku większości popularnych rozwiązań klucz prywatny jest taki tylko z nazwy. Dlaczego? Ponieważ dostawca usługi ma do niego dostęp, a tym samym także do danych. Jeśli dostawca posiada dostęp, to inni też mogą go uzyskać.

W naszej usłudze klucz prywatny posiada jedynie użytkownik, a klucz publiczny przechowywany jest w technologii blockchain. Dodatkowo, wykorzystując metodę „zero-knowledge security” zapewniamy, że dane są w stu procentach prywatne. Oznacza to, że w przypadku utraty danych logowania Cypherdog nie pomoże w odzyskaniu zaszyfrowanych danych ani uzyskania ponownego dostępu do konta, ponieważ nie ma takiej możliwości.

Do potwierdzania tożsamości nie używamy wiadomości SMS, żadnej „zaufanej trzeciej strony”, jak Google, Facebook czy Microsoft ani dostawców podpisów elektronicznych i centrów certyfikacyjnych. W tym celu użytkownik używa kodu QR podczas osobistego spotkania z uczestnikiem wymiany plików i rozmów.

Unikalność naszego rozwiązania poparta jest złożonymi wnioskami patentowymi w USA.



Do jakich przedsiębiorstw kierujecie swoją ofertę?

Klienci Cypherdog należą do wielu sektorów, ponieważ procesy, które chronimy dotyczą w zasadzie wszystkich firm. Niektóre branże są jednak szczególnie narażone na utratę bezpieczeństwa i wizerunku, dla nich ochrona danych jest niewrażliwa. Należą do nich sektor prawny, biura rachunkowe, audytorzy, służba zdrowia, agencje HR i marketingowe, które przetwarzają dane osobowe. Wielu z tych firm dotyczą ścisłe regulacje, takie jak NIS 2, DORA czy ISO 27001/2 – aby działać w zgodzie z nimi, powinny skutecznie szyfrować dane.

Nasze rozwiązanie pomaga też przedsiębiorstwom przeciwdziałać podwójnym wymuszeniom nowej generacji ransomware, w ramach których atakujący nie tylko szyfrują dane, ale także szantażują firmy

ich publikacją, jeśli te nie zapłacą okupu. Dodatkowo zabezpiecza przed invoice hacking oraz business email compromise, czyli płaceniem cyberprzestępcom na podstawie sfałszowanych faktur, rachunków czy innych dokumentów.

Oprócz oferowanej technologii, czy zapewnacie wsparcie w kwestii bezpieczeństwa?

Absolutnie, zależy nam na prawidłowym zabezpieczeniu komunikacji, dlatego pomagamy firmom zidentyfikować dane, które są najistotniejsze oraz procesy, w których uczestniczą. Najprostszy przykład – szereg poufnych dokumentów przesyła się regularnie np. do zewnętrznych firm księgowych czy kancelarii prawnych. Zazwyczaj odbywa się to drogą mailową, a taka komunikacja jest niezabezpieczona. Każda firma powinna zadać sobie pytanie – jakie byłby konsekwencje przechwycenia i wykorzystania tych dokumentów przez konkurencję?

Do identyfikacji kluczowych danych i procesów proponujemy opracowany przez nas "analizator procesów". Ten arkusz, gdy zostanie dokładnie wypełniony, tworzy macierz procesów – wskazuje w jakich działach występują, jakie dane obejmują oraz z jakimi zagrożeniami się wiążą. Identyfikacja oraz zabezpieczenie komunikacji w ramach tych procesów pozwala przeciwdziałać szpiegostwu gospodarczemu oraz wyciekom danych wrażliwych i osobowych, co jest wymogiem m.in. RODO.

W takim razie czy powiedziałbyś, że ekspert i dostawca usług może być przyjacielem?

Według mnie nawet powinien, przecież nasze rozwiązania tworzymy dla ludzi. Jesteśmy, jak to się mówi, "disruptors", bo działamy wbrew aktualnym tendencjom. Dziś największe korporacje masowo zbierają o nas informacje, dane osobiste – nasza działalność polega na ochronie ludzi przed tym, co wydaje się oczywistością nie do zwalczania.

W ostatnim plebiscycie CRN Channel Awards zostaliście laureatem w kategorii "Polski produkt/usługa". Jaki jest Wasz przepis na sukces?

CCypherdog rozwija się zarówno dynamicznie, jak i globalnie. Oprócz Polski, działamy również m.in. w Stanach Zjednoczonych, Izraelu czy Singapurze. Nasz międzynarodowy zespół łączy w sobie energię, talent i zapał młodego zespołu developerów oraz wieloletnie doświadczenie ekspertów, którzy im przewodzą. Są u nas dwa pokolenia, które wspierają i uczą się od siebie nawzajem, tworząc spójny zespół.

Wspólnie osiągnęliśmy już wiele – w 2021 roku zostaliśmy także laureatem plebiscytu "Ambasador Polskiej Gospodarki" organizowanego przez Business Centre Club w kategorii „Kreator Rozwiązań XXI Wieku”. Wyróżnienie to przeznaczone jest dla firm o wysokim stopniu innowacyjności, promujących polską gospodarkę przez ofertę własnych nowatorskich produktów lub usług jeszcze dotychczas w świecie nieoferowanych.

Jakie macie plany na najbliższe miesiące?

Nie spoczywamy na laurach. 25 stycznia wprowadziliśmy nową usługę – token użytkowy CDOG. Będzie go można wykorzystać do opłaty za nasze aplikacje oraz w przyszłości umożliwi zakup innych rozwiązań z obszaru cyberbezpieczeństwa. Chcemy też, żeby nasz token stanowił alternatywną metodę na pozyskanie finansowania – globalną, prostszą niż venture capitals czy anioły biznesu.

Tokeny i kryptowaluty ogółem często kojarzą się z brakiem bezpieczeństwa – ponieważ są nowe, nieuregulowane i najczęściej słyszy się o nich w kontekście cyberataków. Jest to natomiast naturalna kontynuacja rozwoju technologii blockchain i świata krypto, a także działalności naszej firmy.

Na najbliższe miesiące mamy zaplanowany również szereg nowych funkcjonalności – rozbudowujemy naszą usługę o manager haseł, dodajemy do messenger komunikację głosową i wideo, a także wprowadzamy bezpieczny podpis elektroniczny.

Cypherdog należy również do MAIN Partner Community.

Spośród dostępnych kanałów zdecydowaliśmy się na sprzedaż poprzez partnerów. Wybraliśmy ten model, ponieważ gwarantuje on skalowalność – działając z pomocą partnerów docieramy do ich klientów jako zaufana firma. W cyberbezpieczeństwie zaufanie jest podstawą – nic w tym dziwnego, w końcu musimy wierzyć firmie, która ma zabezpieczyć nasze najcenniejsze dane.

Postanowiliśmy dołączyć do MAIN Partner Community, ponieważ znajduje się tam już wiele znanych firm, więc z jednej strony jest to dla nas dźwignia w budowaniu zasięgu, relacji opartych na zaufaniu, ale też możliwość zawiązania ciekawej współpracy i wspólnego tworzenia skutecznych, bezpiecznych i nowoczesnych rozwiązań IT dla firm na całym świecie.

Dzięki naszemu rozwiązaniu MAIN zapewnia klientom pełną poufność komunikacji, na którą składają się m.in.: bezpieczna wymiana plików, korzystanie z prywatnej, szyfrowanej chmury do przechowywania istotnych danych, szyfrowanie zasobów na dyskach i komunikacji tekstowej.



Wywiad przeprowadziła:

Ariadna Pawluk

Content Specialist w MAIN, która z wielką pasją zbliża do siebie światy IT oraz biznesu. Entuzjastka nowych technologii – chmury, konteneryzacji oraz cyberbezpieczeństwa.

Najprostsza droga do chmury

Dostarczamy bezpieczne, łatwo skalowalne rozwiązania chmurowe, dzięki którym możesz skupić się na rozwoju działalności.



MAIN to polska firma specjalizująca się w budowie środowisk chmurowych.

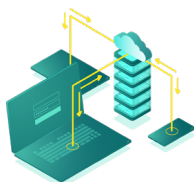
Swoje usługi opiera na sieci własnych ośrodków Data Center w Warszawie. Firma oferuje rozwiązania Private i Hybrid Cloud, uzupełnione konteneryzacją i Disaster Recovery, oraz świadczy wszystkie poziomy administracji środowiskami fizycznymi i wirtualnymi. Wspiera organizacje w pokonywaniu barier, na które natrafiają w związku z przetwarzaniem danych, takie jak niska wydajność czy wysokie koszty infrastruktury.

MAIN jest częścią Grupy EIP.

Produkty i usługi



**Chmura
dla biznesu**



**Zarządzanie
chmurą**



**Serwery
i kolokacja**



**Backup
i replikacja**

Dane kontaktowe MAIN

MAIN Sp. z o.o. | Giełdowa 7/9 | 01-211 Warszawa



ask@main.pl



www.main.pl



+48 (22) 339 18 98

