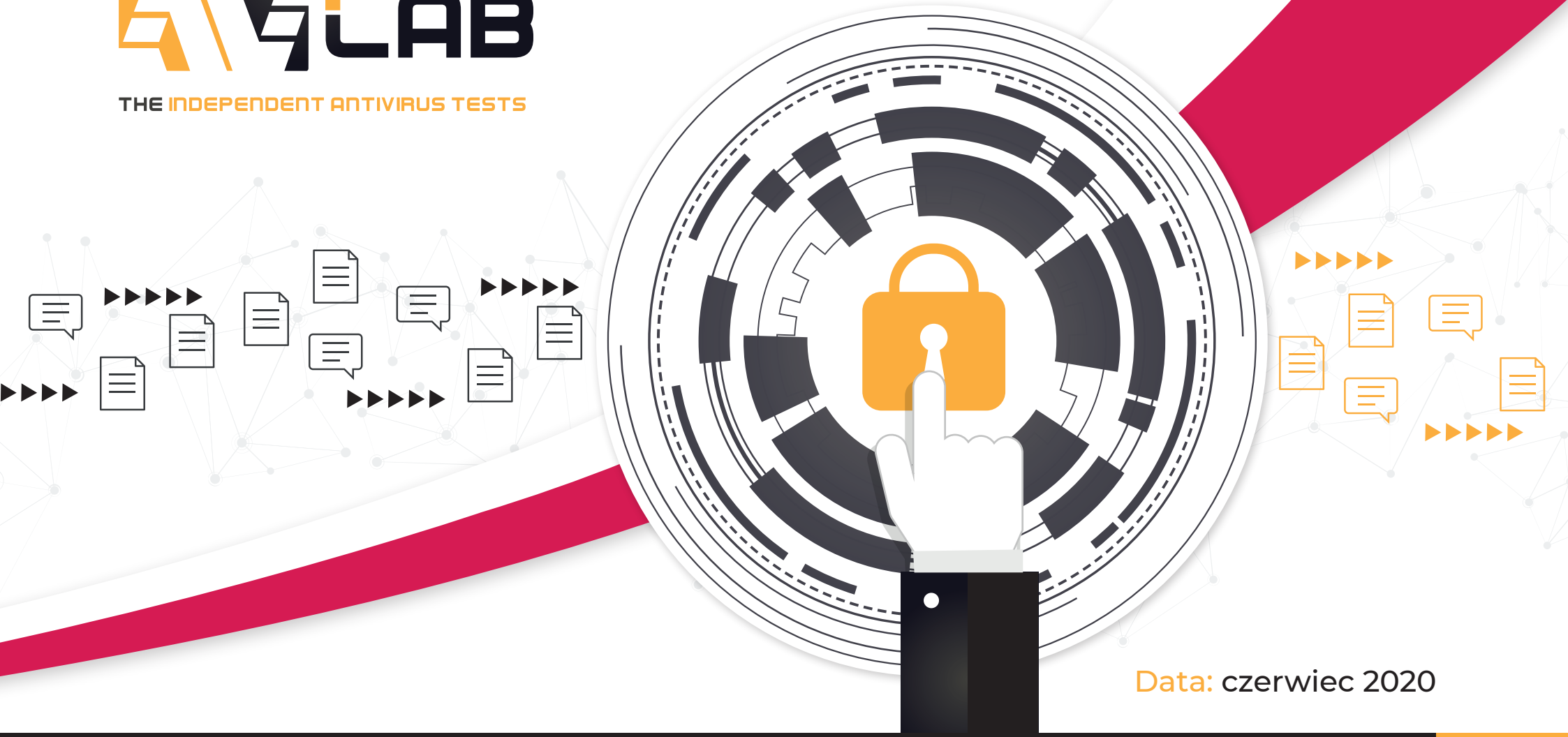
THE INDEPENDENT ANTIVIRUS TESTS

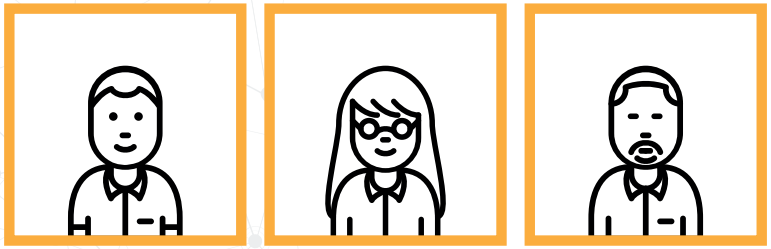


Data: czerwiec 2020

„Made in Poland": porównanie rozwiązań do szyfrowania dokumentów i poufnych informacji

Eksperci są jednomyślni

Szyfrowanie jest jednym z kilku rekomendowanych sposobów zabezpieczenia cyfrowych informacji przed niezaufaną stroną trzecią. Przekształcone dokumenty do postaci niemożliwej do odczytania będą dla hakerów bezużyteczne.



Dzięki kryptografii i matematycznym obliczeniom możliwe jest zaadaptowanie komputerowych danych do bezwartościowego, cyfrowego szumu, zapewniającego ochronę i poufność przetwarzanych plików.

Pojęcia integralności i poufności [1] zostały wytłumaczone w polskiej ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku. Owe określenia determinują sposób obchodzenia się z danymi osobowymi — muszą być przetwarzane z użyciem środków technicznych lub organizacyjnych, aby zapewnić bezpieczeństwo w razie nieumyślnej utraty, fizycznego zniszczenia lub częściowego uszkodzenia. Środkiem organizacyjnym może być pseudonimizacja albo minimalizacja. Środkiem technicznym może być szyfrowanie, które jest metodą technicznie niepodważalną, spełniającą wymóg integralności i poufności danych.

W kontekście RODO przestrzeganie przepisów obowiązuje każdego, kto przetwarza dane osobowe. Dotyczy to największych organizacji prywatnych i państwowych, począwszy od banków i instytucji użyteczności publicznej, a skończywszy na stronach internetowych, które są zarządzane przez osoby prowadzące jednoosobową działalność gospodarczą.

Można więc sformułować przekonanie, że konieczność zapewnienia ochrony danych osobowych zachodzi wszędzie tam, gdzie się one pojawiają.

Najsłabszym ogniwem szyfrowania jest edytowanie odblokowanych dokumentów. Eksperci są zgodni, że niewystarczające zabezpieczenia mogą doprowadzić do utraty informacji. W wyniku udanego cyberataku bądź aktywności złośliwego oprogramowania, osoba, która kontroluje łańcuch ataku, będzie mogła przechwycić odszyfrowane dane. Dodatkowo specjaliści uważają, że szyfrowanie powinno być jednym z kilku kroków do cyfrowego zabezpieczania danych przez ich ujawnieniem, ponieważ gwarantuje ono ochronę przechowywanych kopii zapasowych, jak również pozwala współdzielić dokumenty przy spełnieniu wysokich standardów bezpieczeństwa.

Dzięki szyfrowaniu można uzyskać najwyższy poziom ochrony informacji, przy czym słabym ogniwem dostarczalności zakodowanych plików jest wiarygodność odbiorcy. Nadawca musi mieć pewność i jednocześnie być świadom ryzyka, że odbiorca, któremu zamierza wysłać poufne dokumenty, nie utracił kontroli nad urządzeniem, oraz jest tym, za kogo się podaje. Specjaliści są zgodni, że nikt inny oprócz nadawcy i odbiorcy, nie powinien mieć możliwości odczytania zaszyfrowanych danych. Ten problematyczny aspekt jest ważną kwestią dla osób, które oczekują najwyższych standardów prywatności.

Przedsiębiorcy oraz użytkownicy indywidualni, którzy chcieliby wypróbować wskazane w tym raporcie oprogramowanie do szyfrowania, nie muszą spełniać aż tak surowych wymagań co do wiedzy technicznej o kryptografii. Rozwiązania opracowane przez polskich inżynierów zapewniają autentyczność, tajność oraz funkcjonalność grupowego dzielenia się plikami za pomocą łatwych w obsłudze graficznych interfejsów. Z punktu widzenia organizacji dodatkowym atutem jest możliwość wyboru co do miejsca przechowywania zaszyfrowanych plików, czy chociażby zarządzanie kontami pracowników. Dzięki temu firmy, od małych podmiotów po duże, nie muszą wybierać pomiędzy bezpieczeństwem a prywatnością, ponieważ te obszary zostały dobrze zagospodarowane przez producentów porównywanych rozwiązań.

Oprogramowanie Cypherdog, Specfile oraz Netia Data Safe są gotowe, aby sprostać surowym wymaganiom stawianym przez rozporządzenie o ochronie danych osobowych. Posiadają dodatkowe cechy wspomagające organizowanie i zarządzanie pracą, i jednocześnie gwarantują bezkompromisowe bezpieczeństwo dostępu do plików, w tym prywatność użytkowników oraz tajność przesyłanych informacji.

[1] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf

Dlaczego warto szyfrować?

- Szyfrowanie zataja informacje przed niezaufanymi osobami.
- Szyfrowanie chroni dane przed nieautoryzowanym dostępem z zewnątrz i z wewnątrz firmy.
- Szyfrowanie to dodatkowa ochrona służbowego laptopa i smartfonu.
- Szyfrowanie nie stwarza dodatkowego ryzyka wycieku danych.
- Szyfrowanie jest niezależne od innych zabezpieczeń.
- Wykradzione zaszyfrowane dokumenty nie są wartościowe dla przestępców.

Dla kogo szyfrowanie jest istotne?

Istnieją grupy zawodowe czy też branże, dla których bezpieczeństwo jest kluczowe. Należą do nich osoby odpowiedzialne za finanse spółek, biura rachunkowe, prawnicy, lekarze, sędziowie, adwokaci. Szczególnie chronione powinny być dane osobowe przetwarzane przez służby ratunkowe, policję i banki. Przedsiębiorstwa prywatne oraz instytucje państwowe powinny korzystać z szyfrowania ze względu na poufność dokumentów przetargowych, informacyjnych, projektów badawczo-rozwojowych, ofert i umów handlowych. Bezpieczeństwo informacji dotyczy także osób, które nie zgadzają się na dzielenie się kontaktami i metadanymi z firmami takimi jak Google, Apple, Facebook.

Kiedy szyfrowanie nie jest skuteczne?

- W trybie edycji poufne dokumenty muszą być odszyfrowane.
- Szyfrowanie nie zabezpiecza przed wszystkimi zagrożeniami.
- Ransomware może nadpisać już zaszyfrowane pliki.
- Szyfrowanie nie zapewnia bezpieczeństwa w przypadku awarii nośnika.

Zapamiętaj!

Klucz szyfrowania jest jedyną formą zabezpieczania plików i katalogów. Musisz chronić hasło logowania do aplikacji najlepiej jak potrafisz.

Przechowuj poufne dane w zaszyfrowanych katalogach lub zaszyfrowanych dyskach zewnętrznych.

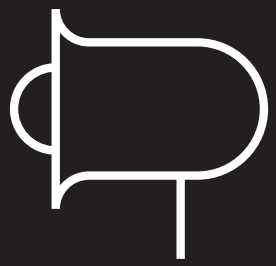
Podłączaj zaszyfrowany dysk do komputera wyłącznie wtedy, gdy pracujesz z ważnymi dokumentami i odłączaj zaraz po zakończeniu pracy.

Odblokowane pliki mogą zostać wykradzione przez hakera albo zniszczone przez złośliwe oprogramowanie.

Oprócz szyfrowania używaj rozwiązania do ochrony przed trojanami i keyloggerami. Aktywny keylogger zmniejsza skuteczność ochrony hasła do klucza prywatnego.

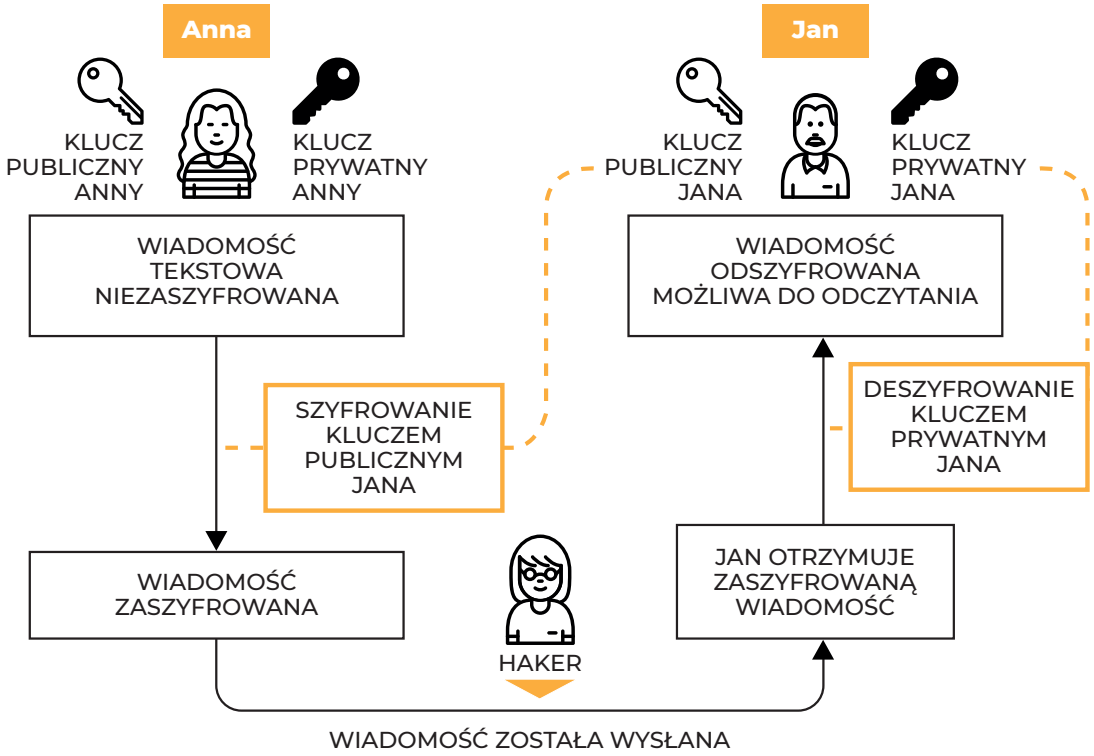
Wyciek danych nie zawsze jest skutkiem cyberataku z zewnątrz. Ktoś z wewnątrz firmy może wykradać dane poprzez przeglądarkę, program pocztowy, komunikator albo zdjęcia wykonane smartfonem.

Zaimplementuj w firmie rozwiązanie DLP (Data Leak Prevention) do ochrony przed niekontrolowanym wyciekiem.



Szyfrowanie oparte o kryptografię asymetryczną

Kryptografia klucza publicznego pozwala ustanowić bezpieczną komunikację, nawet wówczas, kiedy nie ma się możliwości uzgodnienia tajnego klucza z wyprzedzeniem. Jest to ważne dla bezpiecznych transakcji realizowanych przez Internet. Kryptografia z kluczem publicznym zapewnia mechanizm cyfrowego „podpisywania" plików. Pozwala upewnić się co do niezaprzeczalności kontaktów. Posiada jednak wadę: nie daje gwarancji, że wiadomość na pewno pochodzi od nadawcy. Pod rozmówcę może się podszywać ktoś inny, kto wszedł w posiadanie urządzenia. Chociażby z tego powodu należy pamiętać o zabezpieczaniu komputerów, laptopów i smartfonów przed kradzieżą.



W kryptografii asymetrycznej z kluczem publicznym obie strony, które się komunikują, posiadają dwa własne klucze: łącznie cztery klucze. Magia kryptografii klucza publicznego polega na tym, że wiadomość zaszyfrowaną kluczem publicznym, można odszyfrować tylko za pomocą klucza prywatnego, należącego do tej samej pary kluczy. Tak więc, aby wysłać zaszyfrowaną wiadomość do nadawcy, należy posiadać jego klucz publiczny, którym szyfrowane są pliki.

Rozpatrując to na przykładzie:
Jeżeli Anna szyfruje wiadomość za pomocą klucza publicznego Jana i pomimo tego, że haker wie, iż Anna używała klucza publicznego Jana, oraz że haker zna klucz publiczny Jana,to nie jest on w stanie odszyfrować wiadomości. Tylko Jan, używając swojego tajnego klucza prywatnego, może odszyfrować wiadomość od Anny.

Klucze publiczne można ujawniać i wymieniać np. poprzez mail, komunikator, na stronie internetowej lub przekazywać osobiście na pendrive, jednak nie jest zalecane ujawnianie klucza publicznego niepowołanym do tego osobom. Co prawda istnieją graficzne programy do generowania kluczy, ale ich obsługa oraz wymiana z rozmówcą może być problematyczna bez posiadania wiedzy technicznej na odpowiednim poziomie.

Ochrona klucza prywatnego i hasła do aplikacji

Klucz prywatny powinien być maksymalnie chroniony i przechowywany w miejscu niedostępnym, gdyż odszyfrowanie danych powinno być możliwe tylko przez właściciela tego klucza. Ujawnienie klucza prywatnego powoduje, że zaszyfrowane dane mogą zostać rozkodowane (ale nie zawsze).

Producenci rozwiązań Cypherdog, Specfile i Netia Data Safe stosują dodatkowe zabezpieczenia na wypadek kradzieży loginu i hasła do aplikacji. Mogą to być na przykład tak zwane „zaufane urządzenia": wyłącznie te wskazane przez użytkownika albo przez administratora pozwalają na uwierzytelnienie się właścicielowi konta.

Dodatkową kontrolą może być obowiązek zaimportowania kopii klucza prywatnego lub utworzenie konfiguracji ratunkowej. Tylko wówczas możliwe będzie zalogowanie się na innym urządzeniu. Dostawcy rozwiązań zadbali o to, aby niezależne od szyfrowania mechanizmy kontrolne zabezpieczały dane przed niepowołanym dostępem, jeszcze jedną warstwą ochronną.

Jak szyfrować pliki za pomocą Cypherdog, Specfile albo Netia Data Safe?

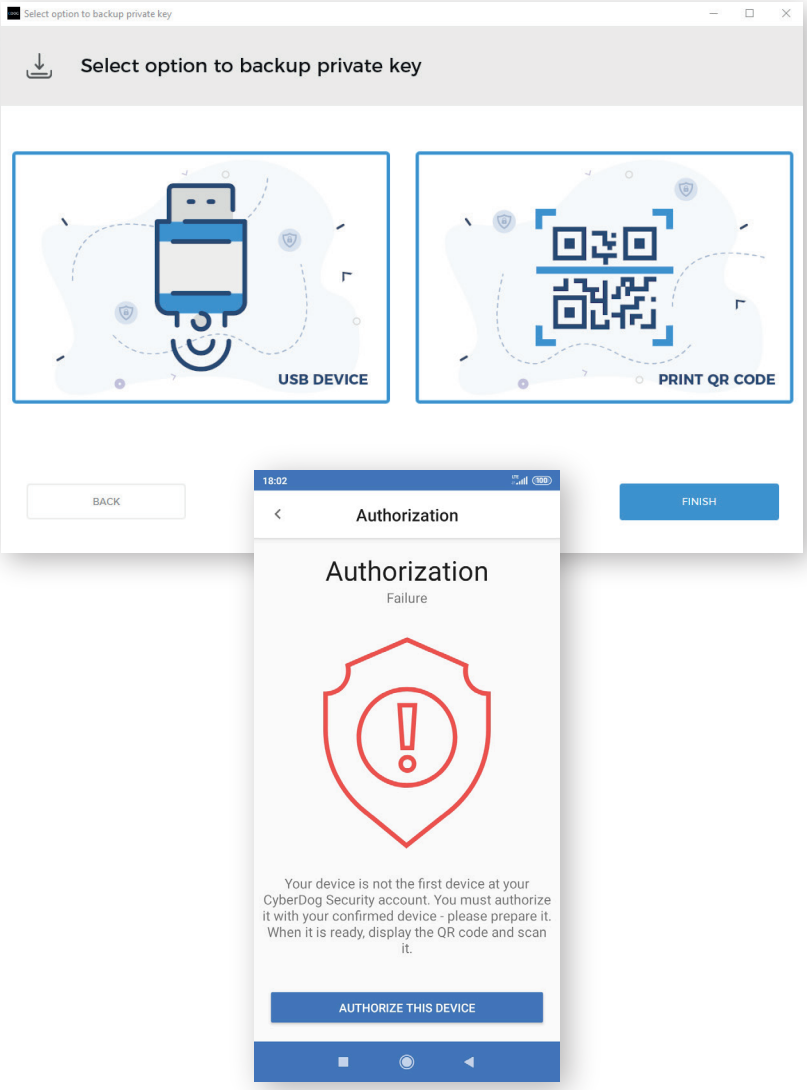
Rozwiązania opisywane w tym raporcie nie wymagają technicznej wiedzy o szyfrowaniu. Co więcej, oprócz automatycznej wymiany kluczy, dodają kolejne warstwy bezpieczeństwa, które nie są dostępne w standardzie kryptografii asymetrycznej.

Użytkownik nie musi nic wiedzieć o generowaniu kluczy i używaniu kryptografii klucza publicznego. Oprogramowanie firm Cypherdog, Specfile, Netia Data Safe są polecane wszystkim przedsiębiorcom, jak i osobom prywatnym ze względu na możliwość pracy grupowej oraz dodatkowe bezpieczeństwo zamknięte w graficznym programie, który nie jest trudniejszy w obsłudze od przeglądarki internetowej. Pod względem technicznym zagadnienia potrzebne do generowania i wymiany kluczy są realizowane przez aplikację, której obsługa jest maksymalnie uproszczona.

CYPHER.DOG™ specfile.pl NETIA Data Safe

Przedstawienie testowanego rozwiązania

CYPHER.DOG™



Dzięki aplikacji możliwe jest wysyłanie plików w dowolnych formatach i rozmiarach w sposób bezpieczny. Wszystkie transfery szyfrowane są w trybie end-to-end. Opracowana technologia i metoda szyfrowania gwarantuje, że nikt z wyjątkiem wskazanego odbiorcy nie jest w stanie odszyfrować transferowanego pliku. Wystarczy dodać odbiorcę do książki adresowej i rozpocząć bezpiecznie transfer plików.

Danych nie jest w stanie nikt odczytać, ani producent, ani żadna inna „trzecia strona". Jednocześnie, dzięki potwierdzeniu tożsamości kontaktów w rejestrze blockchain, użytkownik ma pewność, że nikt nie podszywa się pod osobę, z którą się komunikuje.

Cypherdog, oprócz funkcji szyfrowania w tej samej aplikacji, oferuje czat do rozmów tekstowych z dodanymi kontaktami. Producent zastosował najwyższy poziom prywatności, dzięki czemu rozwiązanie ma zastosowanie w każdej organizacji i dla konsumentów indywidualnych, którzy cenią sobie anonimowość i poufność. Jest szczególnie przydatny w sektorach prawa, finansowym, sprzedaży, medycynie, przemyśle oraz w organizacjach badawczo-rozwojowych.

Pytania do eksperta

Imię i nazwisko: **Przemysław Kucharzewski**
Stanowisko: **VP Sales, Cypherdog Sp. z o.o.**

? W jakich sytuacjach szyfrowanie nie ma wpływu na bezpieczeństwo danych? O czym trzeba pamiętać, przystępując do szyfrowania plików?

Szyfrowanie nie ma wpływu na bezpieczeństwo danych w przypadku celowego lub nieświadomego naruszenia przez ich właściciela podstawowych zasad przechowywania sekretów potrzebnych do autentykacji w systemie przechowującym te dane.
Po wtóre zastosowanie słabych metod szyfrowania również znacząco ogranicza bezpieczeństwo zaszyfrowanych danych. Należy używać unikalnych i mocnych haseł do zabezpieczenia szyfrowania. Wybrać metodę szyfrowania, która zapewni wysoki poziom bezpieczeństwa, o odpowiednich kluczach, przechowywanych w sposób uniemożliwiający ich pozyskanie przez niepowołane osoby.
No i należy też pamiętać o trwałym usunięciu niezaszyfrowanego oryginału (zwykła komenda „delete" nie oznacza jednocześnie, że nie da się pliku odzyskać za pomocą narzędzi do odzyskiwania skasowanych plików).

? Czy praca na odszyfrowanych plikach stwarza zagrożenia dla przedsiębiorstwa? Czego należy unikać i w jaki sposób chronić dane wrażliwe podczas edytowania?

Praca na odszyfrowanych plikach powinna odbywać się jednak na bezpiecznych komputerach należących do przedsiębiorstwa w należycie chronionej sieci lokalnej lub wirtualnej. Szyfrowanie danych jest koniecznością w przypadku przesyłania danych pomiędzy użytkownikami z wykorzystaniem publicznych sieci lub składowania na zewnętrznych serwerach i platformach. Systemy operacyjne dostarczają wystarczająco wysoki poziom zabezpieczeń dla plików przechowywanych lokalnie jak np. dyski szyfrowane za pomocą technologii BitLocker dla Windows lub FileVault dla MacOS. Najsłabszym ogniwem w zabezpieczeniach dysków niezależnie od ich lokalizacji (komputer lub chmura) jest zawsze użytkownik, który nie przestrzega podstawowych zasad polityki bezpieczeństwa przechowywania danych autentykacji.

? W jaki sposób firmy powinny umożliwić pracownikom współdzielenie się plikami, aby robić to zgodnie z kulturą bezpieczeństwa i obowiązującymi przepisami?

W firmowej sieci lokalnej systemy operacyjne, sieciowe usługi katalogowe i scentralizowane usługi autentykacji i autoryzacji są wystarczającymi środkami do budowy dobrze zarządzanych środowisk dla zespołów roboczych. Kultura bezpieczeństwa wymaga jednak by przy transferach danych poza sieć lokalną przedsiębiorstwa bezwzględnie stosować rozwiązania do szyfrowania zarówno kanałów komunikacyjnych jak i samych danych.

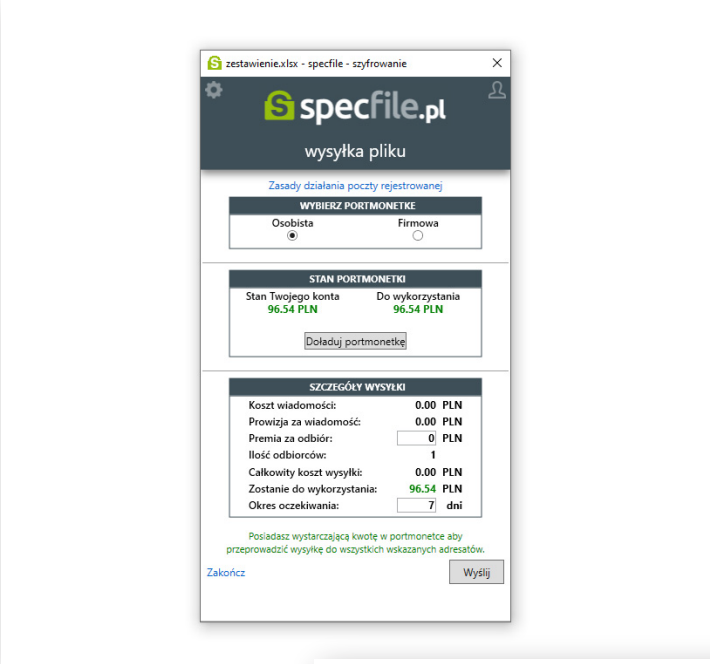
? Czy szyfrowanie może w jakiś sposób wyeliminować problem mieszania się plików i danych służbowych z prywatnymi?

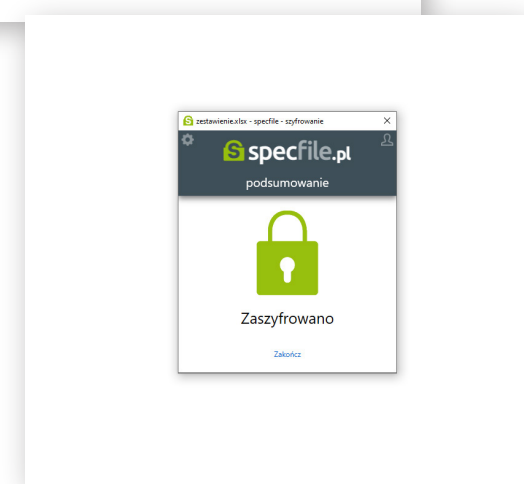
Sama idea „mieszania" się danych prywatnych i firmowych jest zaprzeczeniem podstawowych zasad związanych z zachowaniem poufności danych przedsiębiorstwa. Szyfrowanie w tym przypadku nie rozwiązuje podstawowego problemu braku kontroli przedsiębiorstwa nad swoimi danymi. Dopiero po zapewnieniu pracownikowi środowiska, które bezwzględnie separuje dane przedsiębiorstwa od danych prywatnych można zacząć budować kolejne warstwy zabezpieczeń informacji, jak np. „szyfrowanie w tranzycie".

? Czy szyfrowanie jest wystarczające, aby spełniać wiele wymogów stawianych przez tzw. RODO w kontekście przetwarzania i przechowywania danych osobowych?

Szyfrowanie pomaga spełnić wiele wymogów, ale nie wszystkie. Szyfrowanie jest szczególnie pomocne w zakresie wypełnienia obowiązków przechowywania kopii zapasowej danych wynikających z przepisów związanych z prowadzeniem działalności gospodarczej jak i ustaw o przetwarzaniu informacji powierzonej. Drugim bardzo istotnym zagadnieniem powiązanym z szyfrowaniem jest zapewnienie spójnego systemu autoryzacji dostępu i audytu dostępu do tych danych. Zastosowanie nawet najlepszych metod szyfrowania danych w sytuacji, gdy wszyscy mają dostęp do klucza deszyfrującego jest stwarzaniem jedynie pozorów zachowania poufności, dostępności i integralności informacji.

Przedstawienie testowanego rozwiązania





Specfile pozwala na szyfrowanie danych jednym kliknięciem i wysyłanie tzw. „Elektronicznych Listów Poleconych", czyli odpowiedników tradycyjnej wysyłki rejestrowanej. Jeśli odbiorca odbierze i odszyfruje wysłany plik, nadawca otrzyma e-mail z potwierdzeniem odbioru. Dzięki takiej wymianie informacji zapewniona jest ochrona każdego poufnego pliku przed niepowołanym dostępem. Zabezpieczone w programie dokumenty otrzymują rozszerzenie .spcf, przez co szybko można je zidentyfikować w gąszczu innych plików.

Aplikacja pozwala na bezpieczną wymianę poufnych dokumentów pomiędzy kontrahentami i współpracownikami przez Internet. Specfile wykorzystuje do szyfrowania plików algorytmu kryptograficznego AES z 256-bitowym kluczem. Użyty klucz szyfrowany jest algorytmem RSA z użyciem pary 4096-bitowych kluczy prywatnego i publicznego. Aktualnie nie są znane metody deszyfracji tak szyfrowanych plików bez znajomości kluczy, co zapewnia poufność oraz bezpieczeństwo całym katalogom.

Specfile znajdzie zastosowanie w ochronie patentów, planów know-how, rozliczeń podatkowych, dokumentów spółek i archiwizowania plików. W aplikacji z łatwością odnajdą się osoby nietechniczne, które pracują w biurach księgowych, kancelariach prawnych i adwokackich. Rozwiązanie tego producenta może zabezpieczać wyniki badań pacjentów oraz ich karty w przychodniach i szpitalach. Produkt spełnia stawiane przed nim wymagania wszędzie tam, gdzie personel oczekuje od aplikacji prostoty w obsłudze i intuicyjności w szyfrowaniu.

Pytania do eksperta

Imię i nazwisko: **Katarzyna Abramowicz**

Stanowisko: **Prezes Specfile Project**

? W jakich sytuacjach szyfrowanie nie ma wpływu na bezpieczeństwo danych? O czym trzeba pamiętać, przystępując do szyfrowania plików?

Szyfrowanie nie ma wpływu na bezpieczeństwo danych w wielu sytuacjach: gdy szyfrowanie odbywa się w zainfekowanym systemie, szyfrujemy dane powszechnie dostępne, szyfrowanie zostało zrealizowane w niewłaściwy sposób albo szyfrowanie nie jest łączone z weryfikacją integralności danych oraz mechanizmami pozwalającymi na niezaprzeczalność pochodzenia danych np. podpisem cyfrowym. Ponadto szyfrowanie zostało zrealizowane w systemie o dość przewidywalnym stanie w momencie szyfrowania, co może się przełożyć na słabą jakość danych pseudolosowych użytych do szyfrowania i generowania sekretów, jak i to, że szyfrowanie odbywa się w niezaufanym środowisku którego konfiguracja nie jest w pełni kontrolowana przez szyfrującego. Bezpieczeństwo szyfrowania zagrożone jest wówczas gdy opiera się jedynie na pojedynczym faktorze np. na haśle użytkownika, które jak wiadomo najczęściej posiada niski indeks bezpieczeństwa. Myślę, że warto o tym wiedzieć.

? Czy praca na odszyfrowanych plikach stwarza zagrożenia dla przedsiębiorstwa? Czego należy unikać i w jaki sposób chronić dane wrażliwe podczas edytowania?

Z punktu widzenia oprogramowania pozwalającego na pracę z plikiem .pdf, docx itp, program ten musi widzieć dane pliku, tak jak byłyby jawne. To oznacza że finalnie praca odbywa się na danych jawnych. W naszej aplikacji nie trzeba pamiętać, by zaszyfrować plik po skończeniu pracy.
Zamiast wyliczać kiedy coś jest bezpieczne a kiedy nie jest, lepiej się ograniczyć do wyliczania znanych potencjalnych złych praktyk, zagrożeń dla szyfrowania i elementów systemu, które mogą skompromitować ten proces, a następnie zadbać o to, aby możliwie wszystkie zagrożenia wyeliminować. Można więc wymienić takie sytuacje jak: słaba polityka kontroli dostępu do danych poufnych i jeszcze gorsza jej egzekucja. Sytuacje, gdy do naszego komputera ma dostęp inna osoba albo szyfrujemy dane w środowisku, którego nie kontrolujemy. Ta lista powinna być dużo dłuższa i obejmować wiele aspektów czysto technicznych.

? W jaki sposób firmy powinny umożliwić pracownikom współdzielenie się plikami, aby robić to zgodnie z kulturą bezpieczeństwa i obowiązującymi przepisami?

Ogólnie jest tak, że to użytkownik jest zazwyczaj słabym elementem systemu. Im więcej użytkowników ma dostęp do danego pliku, tym zwiększa się ilość możliwych ogniw zapalnych dla kompromitacji dystrybuowanych danych.
Nie ważne jak bezpieczną politykę ochrony danych stworzymy — zbyt dużo zależy od użytkownika końcowego i jego praktyk przy obchodzeniu się z danymi. Tu bardziej trzeba inwestować w edukację, a nie infrastrukturę.

? Czy szyfrowanie może w jakiś sposób wyeliminować problem mieszania się plików i danych służbowych z prywatnymi?

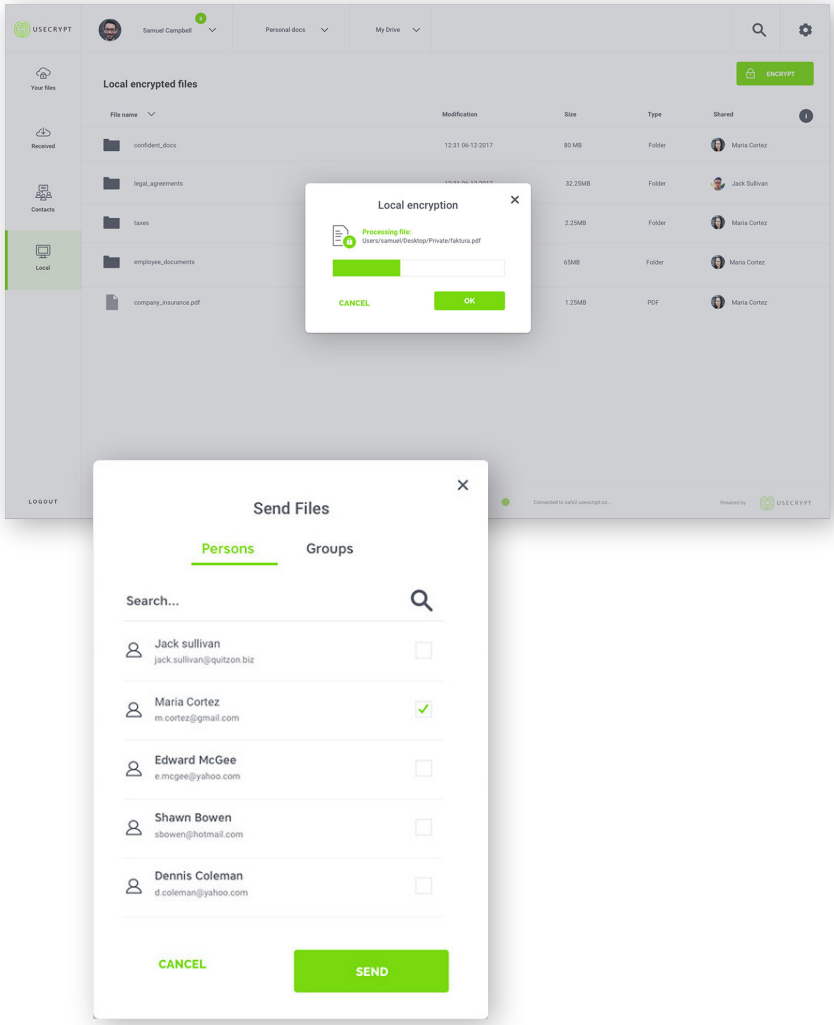
Zależy jaką rolę nadajemy szyfrowaniu. Celem jest zabezpieczyć dokumenty. Naszym zdaniem szyfrowanie może wręcz spotęgować mieszanie się plików. Dużo zależy od ustalonej hierarchii plików i katalogów. Pamiętajmy, że mówimy o oprogramowaniu tylko szyfrującym pliki. Oczywiście można w jakiś sposób pomóc w tym zakresie użytkownikowi, tworząc dedykowany tryb pracy aplikacji np. prywatny i firmowy, i narzucić lub pozwolić mu wybrać katalogi przeznaczone dla tych danych. Aplikacje nie wiedzą czy szyfrują plik prywatny czy służbowy. W większości przypadków użytkownicy wola swobodę w zakresie tworzenia struktury dokumentów na swoim komputerze.

? Czy szyfrowanie jest wystarczające, aby spełniać wiele wymogów stawianych przez tzw. RODO w kontekście przetwarzania i przechowywania danych osobowych?

Na pewno pomaga eliminować ryzyko wycieku treści dokumentów. Pamiętajmy, że szyfrowanie to tylko jeden z wymogów RODO. Jest jednak znacznym podwyższeniem bezpieczeństwa i skutecznym narzędziem dla przeciwdziałania stratom w danych i szkodom dla użytkowników.

Przedstawienie testowanego rozwiązania

N E T I A **Data Safe**



Netia Data Safe to usługa, która zapewnia bezpieczne przechowywanie i współdzielenie danych firmowych dzięki wykorzystaniu innowacyjnych i polskich technologii kryptograficznych, które gwarantują poufność nawet przed dostawcą usługi i producentem oprogramowania szyfrującego.

Rozwiązanie bazuje na innowacyjnej technologii szyfrowania HVKM (Hybrid Virtual Key Management), która polega na podziale prywatnego klucza szyfrującego na dwie odseparowane i przechowywane oddzielnie części. Pierwsza znajduje się na komputerze użytkownika, a druga przechowywana jest bezpiecznie na serwerze. W praktyce oznacza to, że nikt poza właścicielem pliku lub wskazanymi przez niego odbiorcami nie może odszyfrować danych. Producent oprogramowania, albo administrator IT, również nie mają takiej możliwości, ponieważ nie posiadają unikalnej połówki klucza.

Usługa skierowana jest do różnej wielkości podmiotów, w tym m.in. do szpitali i placówek medycznych, kancelarii prawnych i notarialnych, biur rachunkowych, zarządców nieruchomości, firm audytorskich, agencji pośrednictwa pracy i firm head-hunterskich. Rozwiązanie znajdzie zastosowanie wszędzie tam, gdzie ma się do czynienia z koniecznością zabezpieczenia danych wrażliwych, wymagających szczególnej ochrony.

Pytania do eksperta

Imię i nazwisko: **Jakub Sawicki**

Stanowisko: **Kierownik Produktu obszar Cybersecurity**

? W jakich sytuacjach szyfrowanie nie ma wpływu na bezpieczeństwo danych? O czym trzeba pamiętać, przystępując do szyfrowania plików?

Jeśli mówimy o bezpieczeństwie danych, szyfrowanie jest jednym podstawowych i niezbędnych obszarów. Na tak postawione pytanie, mogę z przekonaniem odpowiedzieć, że nie powinniśmy mieć sytuacji kiedy pliki pozostają niezaszyfrowane. Pamiętajmy, że większość dokumentów, na których pracujemy, stanowią wrażliwą lub nawet strategiczną część dla naszego Pracodawcy. Gdyby dostały się w niepowołane ręce, mielibyśmy do czynienia z wyciekiem danych osobowych (RODO i kary z nim związane) lub istotnym naruszeniem wiarygodności czy nawet przyszłości Przedsiębiorstwa (w przypadku gdyby wyciekły projekty czy schematy nieopatentowanych wynalazków). O czym trzeba pamiętać? Przede wszystkim zbadać jakie mechaniki szyfrujące i deszyfrujące są wykorzystane. Można również przestudiować scenariusz, w którym nasze login i hasło zostałyby przejęte (np. wskutek ataku phishingowego czy keyloggera) oraz cyberprzestępca uzyska dostęp do danych i bez problemu je rozszyfruje.

? Czy praca na odszyfrowanych plikach stwarza zagrożenia dla przedsiębiorstwa? Czego należy unikać i w jaki sposób chronić dane wrażliwe podczas edytowania?

Cyberbezpieczeństwo to jedno wielkie ograniczanie możliwości. Określenie mocne, ale najskuteczniejszym sposobem zabezpieczenia naszego biznesu jest utrudnianie życia cyberprzestępcom. Niestety nierzadko wiąże się to z utrudnieniami i ograniczeniami dla naszych użytkowników. Dlatego wszelkie dodatkowe weryfikacje, dodatkowe hasła, dodatkowe aplikacje czy dodatkowe filtry są tutaj stosowane. Jak ocenić przydatność szyfrowania? Wyobraźmy sobie, że nasz komputer służbowy zostaje skradziony. Tragedia? Częściowo tak, ale jeśli korzystamy z backupów, szyfrowania chmurowego i platform zbiorowej pracy na plikach, nie straciliśmy tego co najważniejsze – danych wrażliwych czy strategicznych dla naszej Firmy. Cyberprzestępcy potrafią odzyskiwać dane nawet z komputerów zniszczonych poprzez analizę np. jedynie dysku twardego. Niezaszyfrowane dane odzyskają bez większego problemu. Dobrze zaszyfrowane dane, bez klucza deszyfrującego, zweryfikowanego urządzenia i hasła? Jeśli mają wszystkie komputery świata i kilka miliardów lat na deszyfrowanie...

? W jaki sposób firmy powinny umożliwić pracownikom współdzielenie się plikami, aby robić to zgodnie z kulturą bezpieczeństwa i obowiązującymi przepisami?

Przede wszystkim korzystać z platform, które pozwalają przedsiębiorcy (czyli faktycznego właściciela i odpowiedzialnego za dane) na zarządzanie nimi (przepływem, uprawnieniami), a w razie ich utraty – brak obawy o ich odczytanie przez osoby niepowołane.
Z punktu widzenia samych użytkowników, bardzo wygodne i efektywne są systemy umożliwiające pracę wspólną, wersjonowanie i wzajemne powiadamianie użytkowników o nowych zmianach.
Przypomnijmy sobie ostatni projekt, w którym musieliśmy przygotować dokument, a zmiany wprowadzało kilka osób. Wiele wersji, każdy pracuje na innej. Na koniec kierownik projektu spędza godziny na scalaniu zmian i kreowaniu wersji ostatecznej. Nie wspominam nawet o spamowaniu skrzynek i zapychaniu serwera pocztowego, który przy każdym mailu i każdym adresacie musi przetwarzać i przetrzymywać kolejne zbędne kopie pliku.
Dużą optymalizacją pracy, jest używanie platform pracy wspólnej dla wielu użytkowników jednocześnie i wersjonowania plików.
Jeżeli wszystko jest szyfrowane i zarządzane – mamy komplet.
Jeśli chodzi o przepisy i politykę bezpieczeństwa, zawsze miejmy w głowie regulacje, a w szczególności krótki, ale bardzo znaczący skrót – „RODO", czyli Rozporządzenie o Ochronie Danych Osobowych, na temat którego napisano już niejedną publikację, ale dla nas „zwykłych obywateli", najważniejsze informacje są dwie: „dane należy szyfrować" (to chyba jedno z niewielu technicznych słów występujących w tekście Rozporządzenia) oraz „wyciek danych osobowych oznacza kłopoty i poważne kary".

? Czy szyfrowanie może w jakiś sposób wyeliminować problem mieszania się plików i danych służbowych z prywatnymi?

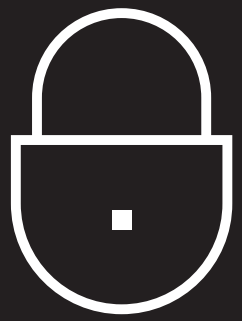
Jak najbardziej! Temat danych prywatnych można rozegrać na kilka sposobów. Jednym z nich jest konteneryzacja, czyli wydzielenie sfery służbowej nawet na urządzeniu prywatnym (BYOD – Bring Your Own Device), która będzie objęta zarządzaniem i monitoringiem bez konieczności ingerowania w sferę prywatną. Można to uzyskać zarówno na urządzeniu mobilnym, jak i PC.
W usłudze Netia Data Safe, taki kontener można utworzyć i utrzymywać automatycznie, czyli utworzyć folder, który z automatu będzie szyfrowany (nawet na zasadzie „drag & drop" – „przeciągnij i upuść").
Dodatkowe narzędzia zabezpieczenia i zarządzania urządzeniami końcowymi (klasy EDR: Endpoint Detection & Response, Endpoint Management & Security) pozwolą wymusić i utrzymać wszelkie polityki bezpieczeństwa, np. „w godzinach 8-17, wszystkie pliki .docx, .xlsx, .pptx zapisuj w folderze szyfrowanym".
Przy odpowiedniej komunikacji wewnętrznej unikniemy sytuacji, kiedy pracownikowi „same zaszyfrują" się jego prywatne dokumenty.
Nie jest to z drugiej strony sytuacja beznadziejna, ponieważ bez nadania odpowiednich uprawnień, nikt (nawet Netia) nie dostanie się do danych.

? Czy szyfrowanie jest wystarczające, aby spełniać wiele wymogów stawianych przez tzw. RODO w kontekście przetwarzania i przechowywania danych osobowych?

Na pewno będzie jednym z najważniejszych elementów. Przedsiębiorca, który wdroży system szyfrowania danych, może mówić o zgodności z wymogami RODO. Samo przechowywanie i przetwarzanie danych będzie zabezpieczone z „użyciem należytej staranności", a „prawo do zapomnienia", które mają wobec wszystkich przedsiębiorców ich klienci (usunięcie wszystkich kopii ich danych osobowych), będzie możliwe do dopełnienia, co nie jest w pełni możliwe, gdy korzystamy z narzędzi publicznych, np. Google Drive, Facebook, Whatsapp, ponieważ nie mamy tam pewności co do finalnego usunięcia danych. Przy Netia Data Safe, każdy przedsiębiorca jest w pełni znaczenia tego słowa właścicielem danych i ma pewność co do nadrzędności przy ich zarządzaniu.
Nie należy jednak zapominać o nieustannym procesie kształcenia użytkowników i udoskonalania polityki bezpieczeństwa. Żaden z systemów nie zapewni 100% bezpieczeństwa, więc część odpowiedzialności (nawet tak mała) leży właśnie na użytkownikach. Nieustannie pracujemy nad rozwojem i jakością oferowanych przez nas rozwiązań, ale nie osiągniemy pełni sukcesu bez współpracy z drugiej strony. Jeśli chodzi o cyberbezpieczeństwo, nie zatrzymujemy się nawet na chwilę, dlatego zachęcam do śledzenia naszych publikacji i informacji, ponieważ ten dynamicznie i nieustannie ewoluujący świat wymaga od nas ciągłej gotowości. Państwo zajmijcie się biznesem, a dbanie o nasze wzajemne bezpieczeństwo zostawcie nam. Od tego jesteśmy!

security by design

privacy by default



Porównanie rozwiązań do szyfrowania i pracy grupowej

BEZPIECZEŃSTWO APLIKACJI I DANYCH

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
MIEJSCE PRZECHOWYWANIA KLUCZA KRYPTOGRAFICZNEGO	Klucz prywatny znajduje się na urządzeniu pracownika. Klucz publiczny wysyłany jest na serwer producenta oraz do sieci blockchain.	Para klucza publiczno-prywatnego po wygenerowaniu na urządzeniu użytkownika jest umieszczana na serwerze producenta, gdzie część prywatna jest zabezpieczona hasłem użytkownika. Zabezpieczona para kluczy jest następnie pobierana przy logowaniu. Producent nie ma dostępu do klucza prywatnego użytkownika.	W wersji standardowej ½ klucza znajduje się na lokalnym komputerze i ½ w chmurze producenta. W wersji dla firm z własnym serwerem ½ klucza znajduje się na lokalnym komputerze i ½ na serwerze firmy.
METODA SZYFROWANIA	AES + RSA + end-to-end	AES + RSA	HVKM + end-to-end + UST + AES + RSA + KDF + DH + MAC + KEM
CZY PRODUCENT MA DOSTĘP DO PLIKÓW PRACOWNIKA?	Nie	Nie	Nie
CZY ADMINISTRATOR W FIRMIE MA DOSTĘP DO PLIKÓW PRACOWNIKA?	Nie	Nie	Nie

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
CZY ISTNIEJE MOŻLIWOŚĆ ODZYSKANIA HASŁA DO KONTA?	**Tak.** Podczas rejestracji użytkownika generowana jest kopia zapasowa klucza prywatnego w postaci czterech kodów QR. Kody te można wydrukować lub umieścić na dysku przenośnym użytkownika. W wersji „Enterprise" dostępna jest dodatkowo opcja archiwizacji kluczy prywatnych w serwisie uruchamianym przez administratora w firmowej sieci lokalnej.	**Nie**	**Tak.** Podczas rejestracji tworzona jest tzw. konfiguracja ratunkowa, która służy odzyskiwaniu dostępu do konta w razie utraty konfiguracji lub hasła.
CZY UJAWNIENIE LOGINU I HASŁA STWARZA ZAGROŻENIE UTRATY PLIKÓW?	**Nie.** Dopiero utrata jednocześnie loginu i hasła do profilu oraz hasła do klucza prywatnego wraz z urządzeniem lub pliku z backupem klucza lub zaszyfrowanego klucza stwarza zagrożenie utraty plików	**Tak.** Należy bezwzględnie zadbać o ochronę hasła do konta.	**Nie.** Do zalogowania się na innym komputerze wymagane są dodatkowe mechanizmy kontrolne (patrz opis poniżej).
CZY APLIKACJA ZOSTAŁA PODDANA AUDYTOWI BEZPIECZEŃSTWA?	**Tak.** Przeprowadzono audyt wewnętrzny. Wykonanie zewnętrznego audytu bezpieczeństwa jest zaplanowane na 3 kwartał 2020 roku.	**Tak.** Aplikacja była poddana zewnętrznemu audytowi systemu kryptograficznego przez zakład kryptografii Wojskowej Akademii Technicznej oraz dwukrotnie audytowi użyteczności.	**Tak.** Przeprowadzono zarówno audyt wewnętrzny (silniki badania podatności wykorzystywane przez Netia Security Operations Center), jak i audyt zewnętrzny przez Deloitte polegający na próbie włamania.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
CZY MOŻLIWE JEST ZALOGOWANIE SIĘ NA INNYM KOMPUTERZE TYM SAMYM LOGINEM I HASŁEM?	**Tak.** Wymagana jest jednak migracja klucza prywatnego użytkownika. Migracja klucza prywatnego na nowy komputer możliwa jest za pomocą procedury odzyskiwania klucza przy pomocy kopii zapasowej. W wersji Enterprise klucz może zostać opcjonalnie odzyskany ze specjalnego serwisu kontrolowanego przez administratora w lokalnej sieci firmowej, o ile taki serwis zostanie skonfigurowany i uruchomiony.	**Tak.** Trzeba jednak bezwzględnie zadbać o ochronę hasła do konta, ponieważ nie istnieją dodatkowe mechanizmy zapobiegające zalogowaniu na innym urządzeniu.	**Tak.** Do zalogowania się wymagany jest plik konfiguracyjny tworzony podczas zakładania konta oraz dodatkowa autoryzacja. Bez autoryzacji nowego urządzenia nie jest możliwe zalogowanie się na innym komputerze.
CZY INFRASTRUKTURA I SERWER, MIEJSCE PRZECHOWYWANIA DANYCH I KLUCZY BYŁY AUDYTOWANE?	**Tak.** Przeprowadzono audyt wewnętrzny. Wykonanie zewnętrznego audytu bezpieczeństwa jest zaplanowa-ne na 3 kwartał 2020 roku.	**Tak.** Brak szczegółowych informacji.	**Tak.** Dane oraz połowa klucza RSA (patrz pkt. 1 dot. podziału klucza) jest umiejscowiony w Netia Data Center, w którym wykorzystany jest szereg technologii i zabezpieczeń (Data Center poziom - Tier III).

Porównanie rozwiązań do szyfrowania i pracy grupowej

FUNKCJE UŁATWIAJĄCE KORZYSTANIE Z APLIKACJI

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
CZY WYMAGANY JEST DOSTĘP DO INTERNETU PODCZAS SZYFROWANIA LUB DESZYFROWANIA PLIKU?	**Tak.** Należy zalogować się do aplikacji. Dostęp do Internetu jest potrzeby m.in. w celu potwierdzenia zgodności klucza publicznego nadawcy ze wszystkimi dostępnymi repozytoriami.	**Nie.** Nie jest wymagane połączenie z Internetem, aby szyfrować i deszyfrować pliki na komputerze. Natomiast bez połączenia niektóre funkcje będą ograniczone.	**Tak.** Internet jest bezwzględnie wymagany (zarówno przy szyfrowaniu jak i deszyfrowaniu), ponieważ ½ klucza deszyfrującego znajduje się na komputerze pracownika i ½ na serwerze firmowym (w wersji on premise) lub producenta (w wersji cloud).
CZY ADMINISTRATOR LUB WŁAŚCICIEL KONTA MA MOŻLIWOŚĆ ODBIERANIA PRAWA DO UDOSTĘPNIONEGO ZASZYFROWANEGO PLIKU?	**Nie.** Administrator może natomiast wyłączyć konto pracownikowi w wersji Cypherdog Enteprise.	**Nie**	**Tak.** Możliwe jest zarządzanie kontami użytkowników przez administratora. Administrator może zarządzać plikami pod warunkiem, że ma do nich uprawnienia.
W JAKI SPOSÓB ODSZYFROWAĆ LUB SZYFROWAĆ PLIKI?	Za pomocą aplikacji Cypherdog.	Za pomocą aplikacji Specfile albo na stronie internetowej producenta.	Za pomocą aplikacji Netia Data Safe.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
MIEJSCE SZYFROWANIA LUB DESZYFROWANIA PLIKÓW	W aplikacji na komputerze pracownika za pomocą interfejsu graficznego lub wiersza komend.	Na komputerze pracownika z użyciem prawego przycisku myszy lub aplikacji albo na stronie internetowej producenta.	W aplikacji na komputerze pracownika lub w obszarze chmurowym w przypadku pracy grupowej.

Porównanie rozwiązań do szyfrowania i pracy grupowej

PLANOWANIE PRACY GRUPOWEJ

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
WSPÓŁDZIELENIE ZASZYFROWANYCH PLIKÓW Z PRACOWNIKAMI	**Tak.** System wspiera jedynie mocne szyfrowanie end-2-end bez wyjątków. Istnieje możliwość przesyłania zaszyfrowanych plików pomiędzy dwoma użytkownikami Cypherdog. Plik może zostać odszyfrowany jedynie przez jednego adresata. Brak zbiorowego dostępu w ramach „grup roboczych”.	**Tak.** W momencie szyfrowania dokumentu można określić osoby, które będą miały dostęp do pliku. Wystarczy podać adresy e-mail. Nie zarejestrowany odbiorca otrzyma zaproszenie i będzie musiał założyć konto, aby odczytać plik. Automatyczny dostęp do pliku uzyskują administratorzy w firmie.	**Tak.** Dzielenie się danymi możliwe jest w sposób maksymalnie bezpieczny w ramach utworzonych grup ze współpracownikami. Tylko uprawnieni użytkownicy mają dostęp do plików. Jeśli uprawnienia zostaną wycofane, dostęp do plików nie będzie możliwy.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
CZAT Z PRACOWNIKAMI	**Tak.** Bezpieczny komunikator dostępny jest w wersji Cypherdog Premium i Enterprise (w wersji desktop i mobilnej). Producent nie ma dostępu do przesyłanych komunikatów oraz do informacji o tożsamości rozmówców. Produkt gwarantuje maksymalne bezpieczeństwo.	**Nie**	**Tak.** Bezpieczny komunikator dostępny jest jako osobna aplikacja tego samego dostwcy.
IMPORT KONTAKTÓW Z APLIKACJI SZYFRUJĄCEJ DO KOMUNIKATORA I ODWROTNIE.	Nie jest wymagany. Kontakty synchronizują się automatycznie. Backend systemu przechowuje zaszyfrowaną kopię książki adresowej. Producent nie ma wglądu w listę kontaktów użytkownika.	**Nie**	W standardzie komunikator jest aplikacją mobilną, natomiast Netia Data Safe aplikacją na komputery, dlatego bez integracji np. z Active Directory nie będzie to możliwe.
MIEJSCE PRZECHOWYWANIA ZASZYFROWANYCH PLIKÓW	Zaszyfrowane pliki lub całe katalogi mogą być przechowywane na dysku pracownika, w chmurze producenta lub na serwerach firmy.	Po zaszyfrowaniu pliki znajdują się na komputerze użytkownika. Następnie klient może je przenieść lub skopiować w dowolne miejsce.	Zaszyfrowane pliki lub całe katalogi mogą być przechowywane na dysku pracownika, w chmurze producenta lub na serwerach firmy.
ZARZĄDZANIE UŻYTKOWNIKAMI	**Tak.** Funkcja taka jest dostępna w wersji Cypherdog Enterprise.	**Tak.** Funkcja jest dostępna dla firm.	**Tak.** Funkcja jest dostępna dla firm.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
ILOŚĆ MIEJSCA NA PLIKI PRACOWNIKA	Domyślnie każdy użytkownik aplikacji Cypherdog dostaje 5 GB miejsca na pliki. Istnieje możliwość rozbudowy dostępnego miejsca w chmurze AWS. Nielimitowana powierzchnia na urządzeniu pracownika.	Pliki są przechowywane na komputerze. Ilość miejsca na dane jest uwarunkowana wolną przestrzenią dyskową. Dodatkowo aplikacja zawiera funkcje synchronizacji z np. chmurą. Użytkownik może wskazać katalog lub chmurę do której ma wysłać zaszyfrowany dokument, wówczas aplikacja wyśle do tego miejsca zaszyfrowany dokument. Utworzy się automatyczna kopia zapasowa dokumentu.	W opcji podstawowej jest to 150 GB dla każdego użytkownika. Dodatkowo, w zależności od wariantu, od 500GB do 2TB przestrzeni dla współdzielenia plików ramach wdrożeń niestandardowych. Netia może zaoferować więcej miejsca na dane na życzenie klienta. W przypadku instalacji produktu na serwerach firmowych ograniczeniem jest pojemność dysków po stronie klienta.

Porównanie rozwiązań do szyfrowania i pracy grupowej

DODATKOWE INFORMACJE

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
WSPIERANE SYSTEMY OPERACYJNE	Cypherdog: Windows, macOS, Linux. Cypherdog Messenger: Android, iOS.	Specfile (aplikacja): Windows. Szyfrowanie i deszyfracja bez aplikacji:przez dowolną przeglądarkę we wszystkich systemach.	Netia Data Safe: Windows, macOS. Messenger: iOS, Android.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
UMOWA O GWARANTOWANYM POZIOMIE ŚWIADCZENIA USŁUG SERWEROWYCH (SLA)	Producent oferuje SLA na poziomie 99,9%. System zbudowany jest w oparciu o architekturę wysokiej dostępności dostępną na 6 kontynentach.	**Nie**	Producent oferuje SLA na poziomie 99,9%. SLA w wersji on-premise jest zależne od infrastruktury firmowej.
CENA 1 LICENCJI (MIESIĘCZNA)	16 dolarów* w wersji Premium 8 dolarów* w wersji Enterprise *Możliwe kalkulacje indywidualne	11 zł	Ceny zaczynają się od 60 PLN za: • przestrzeń dyskową w chmurze Netii (od 150 GB dla każdego użytkownika lub 2TB wspólnej przestrzeni) • wsparcie techniczne Przy większej ilości Użytkowników ceny ustalane są indywidualnie.
DOSTĘPNE JĘZYKI W APLIKACJI	Polski, angielski, ukraiński i rosyjski.	Polski	Polski i angielski.
W JAKICH JĘZYKACH DOSTĘPNE JEST WSPARCIE TECHNICZNE I OPIEKA HANDLOWA?	Dedykowany zespół wsparcia technicznego Cypherdog dostępny jest języku polskim i angielskim.	Polski	Dedykowany zespół wsparcia technicznego Netia w języku polskim i angielskim.
CZY ROZWIĄZANIE MOŻE BYĆ UŻYWANE PRZEZ OSOBY NIE PROWADZĄCE DZIAŁALNOŚCI GOSPODARCZEJ?	**Tak**	**Tak**	W ramach oferty niestandardowej Netia może przeprowadzić takie wdrożenie.

Funkcja lub cecha	Cypherdog	Specfile	Netia Data Safe
CZY SZYFROWANIE PLIKÓW MOŻLIWE JEST BEZPŁATNIE, ALE BEZ DODATKOWYCH FUNKCJI?	**Nie.** Aplikacja do szyfrowania jest płatna. W wersji bezpłatnej możliwe jest jedynie odszyfrowanie przesłanego pliku.	**Tak.** Aplikacja do użytku osobistego pozwala na bezpłatne i nieograniczone szyfrowanie plików ale jest pozbawiona dodatkowych funkcji.	**Nie.** Możliwy jest tylko odczyt plików w ramach bezpłatnej licencji.
STRONA INTERNETOWA PRODUCENTA	**https://cypher.dog**	**https://specfile.pl**	**https://www.netia.pl**

Przyznane rekomendacje

Cypherdog

Najwyższa ochrona prywatności.
Bardzo silne szyfrowanie.
Dostępność czatu w aplikacji i dedykowanego komunikatora.
Przemyślane funkcje dla ułatwienia pracy grupowej.
Wsparcie dla wszystkich systemów operacyjnych z Linuksem włącznie.
Zastosowanie technologii blockchain.
Właśnie tak należy projektować nowoczesne rozwiązania do poufnej pracy grupowej.

Specfile

Funkcjonalność szyfrowania i deszyfrowania plików, niezależna od systemu operacyjnego, również przez przeglądarkę. Potwierdzenie nadania i odbioru wysyłki rejestrowanej.
Powiadomienie o oczekującym liście dla osób bez konta.
Współdzielenie szyfrowanych dokumentów z osobami firmowymi i prywatnymi.
Prawdopodobnie jest to najlepsza usługa szyfrowania danych dla ludzi i dla firm, które oczekują prostego w obsłudze rozwiązania.

Netia Data Safe

Rozwiązanie pozwala przechowywać wszystko na serwerach firmy, bez dostępu kogokolwiek z zewnątrz, nawet producenta.
Unikalna technologia podziału klucza szyfrującego HVKM (Hybrid Virtual Key Management).
Zaawansowane funkcjonalności pracy grupowej.
To są znaki rozpoznawcze produktu, który umożliwia zabezpieczenie danych wymagających szczególnej ochrony.

Podsumowanie

Imię i nazwisko: **Adrian Ścibor**

Stanowisko: **Redaktor prowadzący AVLab.pl**

W 2015 roku naukowcy oszacowali, że ówczesny komputer kwantowy potrzebowałby miliarda kubitów, aby złamać szyfrowanie oparte o algorytm RSA o długości klucza 2048 bitów. To znacznie więcej niż 50-80 kubitów, które nawet teraz posiadają supernowoczesne komputery kwantowe. I matematyka raz jeszcze udowodniła, że jest królową nauk: eksperci z elitarnego Uniwersytetu Cornella opracowali model komputera kwantowego[2], który może wykonać takie obliczenia w czasie 8 godzin, ale nie za pomocą miliarda kubitów, lecz „zaledwie" 20 milionów kubitów. To interesująca praca techniczna, bardzo istotna i pokazuje, że w niedalekiej przyszłości mogą powstawać kolejne modele komputerów kwantowych, które o całe rzędy wielkości zmniejszą ilość potrzebnych kubitów do wykonywania działań faktoryzacji. Czy takie urządzenie zostanie opracowane w nadchodzących dekadach?

Za kilkanaście, kilkadziesiąt lat, bezpieczeństwo algorytmu RSA-2048 może zostać podważone. Obecnie często używa się silniejszego szyfrowania niż RSA-2048 np. w bankowości online, komunikatorach internetowych, szyfrowaniu poczty i plików. O większą stawkę toczy się gra pomiędzy państwami. Jeżeli do tej pory używano szyfrowania RSA-2048 do zabezpieczania danych i komunikacji, to za dwadzieścia lat mogą być problemy z utrzymaniem tajemnic z przeszłości.

Szyfrowanie to jeden z podstawowych standardów bezpieczeństwa. Jest powszechnie dostępne, jak i nieskomplikowane w obsłudze. Z tego powodu chcieliśmy Państwu przedstawić polską myśl techniczną w dziedzinie szyfrowania, bez sięgania po oprogramowanie zza granicy.

Informacje zawarte w naszym badaniu zostały omówione we współpracy z inżynierami każdego z producentów. W tym trudnym czasie warto wspierać polskich przedsiębiorców i promować lokalne, i co podkreślamy, dobre rozwiązania, umożliwiające bezpieczną i poufną pracę grupową dla szerokiego zakresu działalności gospodarczych.

[2] https://arxiv.org/abs/1905.09749

THE INDEPENDENT ANTIVIRUS TESTS

AVLab jako niezależna organizacja stojąca na straży bezpieczeństwa w Internecie zajmuje się dostarczaniem informacji z branży poprzez artykuły, relacje ze szkoleń i konferencji. Naszą cechą rozpoznawczą są profesjonalne recenzje i testy bezpieczeństwa.

W testach wykorzystujemy szkodliwe oprogramowanie, narzędzia i techniki obchodzenia zabezpieczeń, które są używane w prawdziwych atakach. Aby zapoznać się z naszą ofertą prosimy odwiedzić strony:

https://avlab.pl/o-nas **https://avlab.pl/wspolpraca**