Polityka bezpieczeństwa danych osobowych
w Przedsiębiorstwie Informatycznym Sponsor 2
P. Kubala, M. Uchwat s.c.
aktualizacja z dnia 2.07.2018

Dane osobowe przetwarzane w Firmie

Przetwarzamy dane osobowe naszych bezpośrednich klientów ale przede wszystkim dane powierzone nam przez naszych klientów w ramach obsługi księgowości oraz kadr i płac w systemie Kubito.

(...)

Dodatkowo Firma obsługuje konta email na Serwerze przy użyciu serwera poczty elektronicznej oraz serwery wirtualne WWW, które potencjalnie także mogą zawierać dane osobowe bezpośrednio w plikach lub bazach danych obsługujących aplikacje webowe.

Miejsce przetwarzania danych

Wszystkie dane umieszczone są na serwerze Public CLOUD w serwerowni firmy OVH w Ożarowie Mazowieckim pod Warszawą.

1. Dane przetwarzane w systemie informatycznym Kubito, będącym produktem wytworzonym i utrzymywanym przez Firmę są przechowywane w bazie MySQL. System Kubito działający na Serwerze służy do obsługi informatycznej księgowości oraz kadr i płac Firmy oraz jej klientów.
2. Dane przetwarzane przez system MOL są przechowywane są w bazie MSSQL.
3. Dane aplikacji webowych oraz dane związane z obsługa serwera poczty elektronicznej są przechowywane w plikach i bazach MySQL.
4. Kopie zapasowe przechowywane są w innej serwerowni firmy OVH, na terenie Unii Europejskiej.

Metody przetwarzania danych osobowych w Firmie

Dane powierzone przez klientów w ramach usługi hostingu (MOL, strony WWW, poczta elektroniczna) są przetwarzane wyłącznie w celu realizacji usługi tj. przechowywania, udostępniania ich zgodnie z parametrami usługi (www, email) oraz tworzeniem kopii zapasowych. Firma ma fizyczny dostęp do tych danych ale nie zapoznaje się z ich strukturą i zawartością, poza uzgodnionymi z klientem przypadkami, kiedy będzie to niezbędne w celu identyfikacji i naprawy nieprawidłowości funkcjonowania usług, w szczególności w celu identyfikacji i likwidowania zagrożeń i naruszeń.

Dane powierzone przez klientów w ramach obsługi systemu Kubito przechowywane są w bazie MySQL i udostępniane operatorom tego systemu do bezpośredniego przetwarzania. (...)

Przetwarzanie danych przez podwykonawcę – OVH

OVH wdraża środki bezpieczeństwa mające na celu zapewnienie ochrony i poufności

przetwarzanych danych osobowych. W ten sposób zapobiega ich zniekształceniu i uszkodzeniu oraz uniemożliwia nieupoważnionym osobom trzecim dostęp do tych danych. OVH odpowiedzialne jest za bezpieczeństwo infrastruktury fizycznej, zapewniając:

1. fizyczne zabezpieczenia uniemożliwiające dostęp nieupoważnionych osób do infrastruktur, na których przechowywane są dane klienta;
2. dyżury pracowników ochrony czuwających nad bezpieczeństwem fizycznym pomieszczeń OVH 24/7/7;
3. system zarządzania uprawnieniami ograniczający dostęp do pomieszczeń oraz danych tylko do osób, które muszą go mieć ze względu na pełnione funkcje i zakres obowiązków;
4. system fizycznego i/lub logicznego odizolowania usług poszczególnych klientów;
5. ścisłe procedury uwierzytelniania użytkowników i administratorów dzięki rygorystycznej polityce zarządzania hasłami oraz wdrożeniu weryfikacji dwuetapowej (przy użyciu YubiKey);
6. procedury i środki umożliwiające monitorowanie wszystkich operacji przeprowadzanych w systemie informacyjnym oraz raportowanie, zgodnie z obowiązującymi przepisami, w przypadku wystąpienia incydentów dotyczących danych klienta.

Udostępnianie danych osobowych klientom

Klienci uzyskują dostęp do swoich danych elektronicznie, poprzez wykupione i udostępnione usługi: WWW, FTP, POP3 lub IMAP4 oraz w przypadku administratorów baz systemu MOL poprzez bezpośredni dostęp do baz danych MSSQL, jednak wyłącznie z użyciem protokołu OpenVPN szyfrowanego weryfikowanym certyfikatem SSL wystawionym przez naszą firmę.

W wyjątkowych wypadkach, w celu szybkiej reakcji w stanach wyższej konieczności istnieje możliwość bezpośredniej współpracy z upoważnionymi operatorami systemu Kubito, w tym także telefonicznej, w trakcie której możemy uzyskać oraz w razie konieczności przekazywać klientom informacje na temat powierzonych przez nich danych osobowych. Lista operatorów wraz z hasłem telefonicznym niezbędnym do identyfikacji musi zostać dostarczona nam przez klienta będącego administratorem danych osobowych – w ramach załącznika do umowy powierzenia przetwarzania danych osobowych.

Kopie zapasowe

Kopie zapasowe plików przechowywanych na serwerze tworzone są codziennie o godzinie 2:20. Tworzona jest kopia przyrostowa, zawierająca jedynie pliki zmienione od czasu utworzenia poprzedniej kopii. Co tydzień, w nocy soboty na niedzielę aktualizowana jest kopia pełna. Kopia pełna oraz 7 ostatnich kopii przyrostowych przechowywane są bezpośrednio na serwerze. Bezpośrednio po utworzeniu kopie przyrostowe przesyłane są przez FTP do innej serwerowni OVH. Co trzy miesiące oraz w przypadkach, kiedy administrator uzna takie działanie za pożądane przesyłane są tam też kopie pełne.

Bezpośrednio przed utworzeniem kopii przyrostowych plików tworzone są

szyfrowane kopie baz danych MSSQL oraz MySQL. Kopie przyrostowe plików zawierają te kopie baz danych. Klucze szyfrujące przechowywane są w sposób uniemożliwiający ich odczytanie przez operatorów OVH. 2 razy w miesiącu tworzone są kopie pełne. W pozostałe dni tworzone są kopie różnicowe baz MSSQL oraz kopie pełne tych tabel w MySQL, które były aktualizowane w ciągu ostatnich 3 dni oraz w niektórych przypadkach, kiedy jest to wykrywalne i uzasadnione z powodu rozmiarów, kopie różnicowe wybranych tabel.

Kopie przechowywane są zwykle co najmniej przez 12 miesięcy, w każdym wypadku nie krócej niż 6 miesięcy. Ze względu na strukturę danych oraz sposób tworzenia i przechowywania kopii nie ma możliwości usunięcia wybiórczo danych z pojedynczej kopii zapasowej. Wszystkie kopie plików i baz danych są usuwane zgodnie z planem tworzenia i przechowywania kopii zapasowych.

Zabezpieczenie antywirusowe

System operacyjny jest zabezpieczony programem ClamAV. Skanowane są na bieżąco pliki użytkowników nadsyłane przez FTP, SMTP oraz wgrywane na witryny WWW za pośrednictwem interpretera PHP.

W przypadku wykrycia wirusa transmisja jest blokowana: w przypadku FTP i PHP plik jest natychmiast usuwany, w przypadku SMTP wiadomość jest odrzucana, jednakże podejrzane wiadomości wykrywane heurystycznie mogą być zachowywane w kwarantannie do analizy przez administratora. Administrator może podjąć decyzję o zaakceptowaniu wiadomości. Powinien w takim wypadku podjąć działania zmierzające do wykluczenia pojawiania się podobnych fałszywych alarmów w przyszłości. Próba wgrania wirusa przez PHP skutkuje blokadą adresu IP intruza na 2 dni.

Definicje oficjalnej bazy wirusów ClamAV aktualizowane są automatycznie co 2 godziny, dodatkowe, nieoficjalne definicje dystrybuowane przez Sanesecurity aktualizowane są co 3 godziny.

Nie udostępniamy innych kanałów wgrywania plików przez użytkowników. Pliki wgrywane przez administratora innymi kanałami skanowane są programami antywirusowymi na lokalnej maszynie administratora lub testowane na witrynie virustotal.com.

Inne zabezpieczenia

Serwer jest zabezpieczony przed atakami DDOS przez infrastrukturę OVH. Serwer FTP oraz SMTP jest zabezpieczony przed atakami słownikowymi poprzez blokowanie na 60 minut każdego adresu IP z którego dokonano nieudanych 8 prób logowania. Dodatkowo serwer SMTP jest zabezpieczony filtrem antyspamowym a serwer WWW filtrem kontekstowym typu Web Application Firewall (WAF). Filtry te, będące autorskimi rozwiązaniami firmy Sponsor2, są na bieżąco aktualizowane i rozwijane w miarę pojawiania się nowych zagrożeń.

Serwer poczty jest zabezpieczony przed atakami słownikowymi mechanizmem bezpośrednio wbudowanym w oprogramowanie. Ustawiono parametry blokujące na 1 godzinę każdy adres IP, z którego dokonano 10 błędnych prób zalogowania w ciągu 10 minut. Serwisy WWW są zabezpieczone przed atakami słownikowymi za pomocą WAF. System pomiaru błędnych logowań jest złożony, analizuje próby logowania w różnych

okresach czasu (1, 2, 5, 10 i 20 minut) blokując stopniowo nieliniowo rosnącą liczbę błędnych prób. Adresy IP blokowane są minimum na 30 minut. System kubito posiada także zabezpieczenie przed atakiem słownikowym, blokując konta użytkowników na 60 minut w przypadku 10 lub więcej nieudanych prób logowania w dowolnie długim czasie.

Analiza zagrożeń i metody zabezpieczenia danych

Zabezpieczenia infrastruktury fizycznej stosowane przez OVH oraz rozdzielenie miejsca przechowywania kopii i danych podstawowych zapewniają wysoki poziom bezpieczeństwa wobec zagrożeń losowych typu klęski żywiołowe oraz kradzież danych przez osoby nieupoważnione.

Zgodnie z umową z OVH, pracownicy OVH nie mogą uzyskiwać dostępu do danych klienta. Dlatego istnieje niewielkie ryzyko kradzieży danych przez osoby upoważnione (techników OVH). Dla zminimalizowania tego ryzyka kopie wszystkich baz danych, własnych oraz powierzonych przez klientów, są szyfrowane. Szyfrowane są też tabele systemu Kubito zawierające dane osobowe. Technicy nie mają bezpośredniego dostępu do kluczy szyfrujących, ich uzyskanie wymagałoby dekompilacji komponentów systemu Windows, co, choć teoretycznie możliwe, uznajemy za znikomo prawdopodobne.

Zakładamy, że pliki są dostępne przez www lub email, więc nie szyfrujemy ani ich, ani ich kopii. Ewentualne szyfrowanie tabel w bazach danych tworzonych przez klientów pozostawiamy kompetencjom klientów.

Dostęp do baz danych aplikacji webowych możliwy jest wyłącznie z lokalnego hosta. Dostęp do baz danych systemu MOL możliwy jest dodatkowo z zewnątrz, jedynie dla upoważnionych klientów, poprzez OpenVPN, zabezpieczony certyfikatami SSL wystawianymi przez naszą Firmę.

Dane wprowadzane do systemu Kubito przez poszczególnych klientów są niedostępne dla pozostałych klientów i chronione systemem haseł. System umożliwia zaimplementowanie polityki bezpieczeństwa dotyczącej złożoności oraz częstotliwości wymuszania zmiany haseł, której parametry pozostawiamy poszczególnym klientom. Ryzyko przejęcia haseł i danych poprzez podsłuchanie transmisji chronione jest poprzez dostęp do systemu Kubito wyłącznie protokołem https (zabezpieczonym certyfikatem SSL wystawianym przez publiczną firmę certyfikującą). Minimalizację ryzyka przejęcia danych klienta przetwarzanych bezpośrednio w jego zasobach po podaniu hasła, np. poprzez podglądnięcie na komputerze operatora pozostawiamy klientom. W celu zminimalizowania takiego ryzyka system umożliwia zdefiniowanie maksymalnego czasu bezczynności, po którym operator jest automatycznie wylogowywany. Dodatkowo klienci powinni zabezpieczać maszyny wygaszaniem ekranu z blokadą hasłem, jednak ustawienie parametrów komputerów klientów pod tym względem jest poza naszym zasięgiem, pozostawiamy to klientom do samodzielnego skonfigurowania. Ataki słownikowe blokowane są globalnym zabezpieczeniem opisanym w rozdziale „inne zabezpieczenia”, klienci nie mają możliwości zmiany parametrów tego zabezpieczenia.

(...)