Cyberdefence 24

aut. Andrzej Kozłowski 07.11.2017

NOWE WYMOGI W ZAKRESIE OCHRONY DANYCH. SZYFROWANIEM ROZWIĄZANIEM

Zbliżającą się wielki krokami data 25 maja 2018, czyli wejścia w życie RODO w Polsce nakłada szereg nowych obowiązkowych dla firm. Ich właściciele zadają sobie pytania jak nie narazić się na ogromne straty finansowane i uniknąć odpowiedzialności karnej.

RODO wejdzie w życie 25 maja 2018 roku. Obecnie w administracji rządowej trwają prace związane z dostosowaniem polskiego prawodawstwa do wymogów nowej regulacji. Problem ten musi rozwiązać również sektor prywatnym, ponieważ w innym wypadku naraża się na ogromne straty sięgające, zależnie od tego, które przepisy zostały naruszone od 10 do 20 milionów euro lub od 2 do 4 % światowego obrotu przedsiębiorstwa. Z artykułu 32 rozporządzani można wywnioskować, że najprostszą i najbezpieczniejszą metodą ochrony danych jest szyfrowanie. Rządowe Centrum Systemów Informacyjnych Ochrony Zdrowia wydało rekomendacje w sprawie przygotowania się na zmiany związane z RODO.

Czytaj więcej: UseCrypt – jak polska technologia HVKM może zmienić zasady konstrukcji systemów bezpieczeństwa

Zdaniem autorów tego dokumentu szyfrowanie w chmurze jest najlepszym sposobem na pełną ochronę danych na etapie gromadzenia, przetwarzania oraz transmisji danych między komputerami. Zaleca się wybieranie algorytmów szyfrowania, długości kluczy i praktyki stosowanie zgodnie z najlepszymi praktykami. Właściwe zarządzanie kluczami wymaga bezpiecznych procesów generowania, przechowywania, archiwizacji, odzyskiwania, dystrybucji, wycofywania i niszczenia kluczy kryptograficznych. Co więcej technologia kryptograficzna powinna umożliwiać podział kluczy prywatnych użytkownika i zawierać takie mechanizmy, które uniemożliwiają uzyskanie dostępu do danych przez osoby nieuprawnione nawet w przypadku, gdy zostaną przejęte dane uwierzytelniające. Ponadto autorzy dokumentu twierdzą, że użytkujący urządzenie przenośne powinien, jeżeli to możliwe, zastosować odpowiednie środki kryptograficzne wobec przechowywanych na nim danych osobowych i danych medycznych. W szczególności musi wykorzystywać systemy informatyczny umożliwiający szyfrowanie lokalne przy jednoczesnym zastosowaniu technologii podziału kluczy szyfrujących. Kryteria te spełnia UseCrypt produkt polskiej firmy CryptoMind S.A.

USECRYPT

Techniczne zabezpieczenie danych w RODO/GDPR

RODO GDPR	Szyfrowanie plików i folderów	Szyfrowanie end-to-end encryption	Możliwość odzyskania plików	Zaszyfrowany przesył plików	Bezpieczne i zgodne współdzielenie danych	Szyfrowana archiwizacja	Szyfrowany back'up	Pełna rozliczalność dla ADO	GWARANCJA PEŁNEJ POUFNOŚCI: Brak dostępu do danych usługodawcy	GWARANCJA PEŁNEJ POUFNOŚCI: Możliwość wyłączenia dostępu do danych Administratorow IT
UseCrypyt	+	+	+	+	+	+	+	+	+	+
Bitlocker	-	-	-	-	-	-	-	+/-	-	+
Deslock+	+	-	-	-	+/-	-	+	-	-	+
Veracrypt	+	-	-	-	-	-	-	+/-	+	-
Onedrive	-	-	+	+	-	-	-	+	-	-
PGP	+	+	-	+	+	-	-	-	+	+

UseCrypt S.A.
ul. Twarda 18
00-105 Warszawa

(+48) 22 213 96 44
office@usecrypt.com
www.usecrypt.com

Fot. CryptoMind

Czytaj więcej: [Co sprawia, że polski komunikator UseCrypt Messenger jest tak bezpieczny?]