Warszawa, 04.08.2020 r.

Czy chronisz swoje dane w chmurze?

Ułatwienie pracy czy jedynie większe ryzyko otrzymania kary?

Praca w środowisku chmurowym może zaoferować organizacjom wiele korzyści, jak również niesie ze sobą wiele niebezpieczeństw, np.:

- możliwość przechwycenia kont pracowników,
- nieuprawniony dostęp do danych znajdujących się w chmurze,
- nieautoryzowane zmiany czy utrata plików,
- inne naruszenia ochrony danych osobowych.

Wprowadzając odpowiednie polityki oraz procedury nadawania dostępu możemy uniknąć przydzielenia zbyt szerokich uprawnień pracownikowi niższego szczebla czy kontrolować życie konta po odejściu od nas pracownika. Dokumenty powinny być wdrożone po przeprowadzeniu audytu oraz oceny ryzyka, ponieważ dla każdej organizacji inne zabezpieczenia mogą okazać się przydatne.

Niemniej każda organizacja powinna mieć jasne zasady postępowania z nieaktywnymi kontami, nie tylko w chmurze. Zasady te powinny być stosowane, a nie widoczne jedynie na papierze. Wystarczy przypomnieć karę w wysokości 400.000 EUR nałożoną na szpital w Portugalii[1], w którym lekarze mieli za duży dostęp do danych, a ich konta były aktywne nawet po rozstaniu się z pracodawcą. Podobnie wyglądała sprawa szpitalu w Holandii[2], w którym pracownicy mieli dostęp do akt medycznych pewnej celebrytki, mimo iż nie powinni mieć do nich wglądu. Zarzucono szpitalowi brak możliwości wykrycia nieautoryzowanego dostępu do plików oraz brak uwierzytelniania dwuskładnikowego.

Stosując odpowiednie zabezpieczenia techniczne i środki organizacyjne w celu ochrony danych znajdujących się w chmurze, możemy uratować nie tylko finanse naszej organizacji, ale również ustrzec się przed negatywnym PR i utratą zaufania przez aktualnych oraz potencjalnych klientów.

Przykładowo można zastosować następujące środki bezpieczeństwa:

- kontrola dostępu, w tym zarządzanie kontami użytkowników,
- firewall i inne zabezpieczenia zapewnione przez dostawcę chmury,
- szkolenie pracowników, by podnieść ich świadomość i uchronić przed własnymi błędami lub zagrożeniami z zewnątrz,
- wdrożenie odpowiednich procedur.

Chrońmy nasze konto

Człowiek od zawsze stanowi najsłabsze ogniwo każdego systemu bezpieczeństwa. Dlatego należy go szkolić oraz ostrzegać przed aktualnymi kampaniami phishingowymi. Pracownik powinien również wiedzieć, jakie są zasady ustalenia silnego hasła i czy może korzystać z narzędzi do zapamiętywania haseł. Ale ochrona dostępu do konta to nie tylko zadanie pracownika. Organizacja powinna zadbać o uwierzytelnianie dwuskładnikowe, które jest dostępne u większości dostawców chmurowych. Jak pokazały powyższe kary, organizacja powinna również świadomie przyznawać dostępy do dysków

[1] https://www.cnpd.pt/home/decisoes/Delib/20_984_2018.pdf
[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers

iSecure Sp. z o.o. | www isecure.pl | fax +48 22 378 26 34 | Sąd Rejonowy dla m. st. Warszawy w Warszawie
ul. Sienna 72A lok. 214 | e-mail kontakt@isecure.pl | NIP 525-247-17-82 | XII Wydział Gospodarczy
00-833 Warszawa | tel +48 22 126 58 54 | REGON 14-22-29-729 | KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

czy folderów, nadzorować zakres dostępu czy przyznane uprawnienia w środowisku chmurowym. Jest to szczególnie ważne, gdy mamy grupowy dostęp do udostępnionych folderów, aby dokumenty znajdujące się na wspólnym dysku uchronić przed skasowaniem, gdy zawartość jest cenna dla organizacji, a ma do niej dostęp 100 różnych pracowników, w tym pracujących zdalnie. Należy również pamiętać, by regularnie weryfikować uprawnienia dostępowe aktywnych użytkowników czy systematycznie usuwać dostęp do konta po odejściu pracownika.

Sprawdźmy dodatkowe zabezpieczenia na naszym koncie

Często z pakietem chmurowym otrzymujemy domyślne zabezpieczenia od dostawców. Powinniśmy je za każdym razem przejrzeć i uruchamiać dodatkowe, które są nam zapewnione przez dostawcę. Ustawienia bezpieczeństwa i kontroli zapewniane przez dostawcy usług w chmurze często obejmują:

- uwierzytelnianie wieloskładnikowe,
- zarządzanie urządzeniami przenośnymi,
- specjalistyczne narzędzia do zarządzania,
- monitoring aktywności kont,
- ustawienia odpowiednich alertów,
- zabezpieczenia przed utratą danych,
- ochronę przed malware, spamem oraz spoofingiem i phishingiem.

Tak samo jak zabezpieczenie chmury, ważne jest odpowiednie zabezpieczenie komputerów pracowniczych czy naszych punktów dostępowych do Internetu. Często routery mają ustawione domyślne hasła, dzięki czemu niepowołane osoby mogą dostać się do naszej sieci. Trzeba też pamiętać, by mieć odrębną sieć do pracy, a odrębną np. dla gości czy nawet pracowników korzystających z prywatnych urządzeń np. podczas przerw. W związku z powyższym organizacja powinna przeprowadzać regularne przeglądy bezpieczeństwa swoich urządzeń oraz systemów, w tym dbać o ich aktualizację.

Jakie dane przechowujemy w chmurze?

Punkt, który powinien być na samym początku. Przed rozpoczęciem współpracy z dostawcami chmurowymi i wysłaniem danych organizacji do chmury należy zastanowić się, co będziemy w niej trzymać. Musimy mieć świadomość, czyje dane i w jakim zakresie, dla wygody i szybkości pracy, będą dostępne w chmurze, a które niekoniecznie muszą być wysyłane. Gdy już wiemy, jakie dane chcemy wysłać, powinniśmy sobie zadać kolejne pytanie – jak je oficjalnie zaklasyfikować, czy część z nich będziemy regularnie usuwać, jakiej grupie pracowników jaki dostęp przyznamy oraz jak duże uprawnienia będą posiadać użytkownicy chmury. Jeżeli wcześniej nie zaplanujemy procesu przeniesienia danych do chmury, powstanie jedna wielka nieuporządkowana masa danych. A bałagan bywa złym doradcą w zakresie ochrony bezpieczeństwa informacji. Jednak, gdy zorientujemy się, że uprawnienia są zbyt szeroko przyznane lub nie odcięliśmy dostępu byłym pracownikom – może być już za późno.

Dlatego opanujmy chaos plików elektronicznych. Nie przyjmujmy założenia „wrzucam dane do chmury i zapominam o wszystkim", bo przecież dostawcy rozwiązań chmurowych zapewniają, że ich usługi są bezpieczne. Bezpieczeństwo zależy przede wszystkim od świadomości całej organizacji, wiedzy jakie dane posiada w chmurze i kto ma do nich dostęp. Nie należy także zapominać o pracownikach, dostarczając im odpowiednie narzędzia do pracy, klarowne instrukcje związane z bezpieczeństwem i higieną pracy oraz zapewniając im adekwatne szkolenia i zdrowe, owocowe poniedziałki 😊

Przemysław Siarka,
Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł