Problemy z aplikacją ZOOM - czyli jak bezpieczeństwo przegrało z wygodą (UX)

W związku z izolacją, jaka objęła ludzi na całym świecie w kontekście pandemii, coraz większą popularnością cieszą się aplikacje do zdalnej komunikacji. Dotyczy to przede wszystkim tych rozwiązań, które pozwalają na organizację webinarów i telekonferencji. Jedna z nich – ZOOM Cloud Meetings, zyskała szczególną popularność i trafiła w centrum zainteresowania. Niestety nie ze względu na intuicyjną i prostą obsługę, ale problemy z bezpieczeństwem. Można powiedzieć, że ZOOM padł ofiarą własnego sukcesu. Ta historia powinna dać jednak do myślenia również użytkownikom, których złe przyzwyczajenia są głównym źródłem podatności na cyberzagrożenia.

Gdzie tkwi problem?

Zarówno amerykańskie FBI jak i brytyjskie Ministerstwo Obrony ostrzegało przed korzystaniem z ZOOMa od jakiegoś czasu. Jeszcze wcześniej w sieci pojawiły się głosy ekspertów od cyberbezpieczeństwa, którzy zwracali uwagę na zagrożenia jakie stwarza aplikacja. Głównym powodem była podatność na cyberataki i niewystarczająca ochrona prywatności. Dotyczyło to m.in. możliwości nieuprawnionego logowania do trwających telekonferencji, zbyt słabych haseł, których przełamanie dawało możliwość uzyskania dostępu do danych użytkownika czy wysyłania danych o urządzeniu i jego lokalizacji do Facebooka w celu personalizacji marketingowej (bez względu na to, czy użytkownik logował się do aplikacji kontem na Facebooku, bez poinformowania o tym). Dodatkowo użytkownicy korzystający ze skrzynek pocztowych o takiej samej domenie (adresie po @) byli automatycznie dodawani do listy kontaktów, co prowadziło do ujawnienia ich danych osobowych zupełnie obcym osobom.

Producent aplikacji przygotował już aktualizację, która miała wyeliminować podatność ZOOM, pozwalającą na przejęcie kamery i mikrofonu na komputerach MAC. Nie znaczy to, że użytkownicy komputerów z systemem WINDOWS mogą czuć się bezpiecznie – wysyłanie linków na czacie może nadal dawać furtkę dla hakerów do przejęcia nazwy i hasła do urządzenia[1]. Co do szyfrowania transmisji – ZOOM przyznał otwarcie, że nieporozumieniem jest przyjęcie, że szyfrowanie jest pełne.

Mimo opisanych problemów liczba użytkowników aplikacji wzrosła lawinowo. Z aplikacji korzystał nawet brytyjski rząd organizując z jej wykorzystaniem spotkania. Jak widać popularność ZOOM dotyczy nie tylko osób prywatnych czy firm. Pojawia się jednak pytanie, czy opisana sytuacja jest wyłącznie problemem producenta. Jakie wnioski powinniśmy wyciągnąć dla siebie jako użytkownicy tego typu rozwiązań?

Czego (nie)wymagamy od darmowych rozwiązań?

Przyjęło się powszechnie, że od darmowych aplikacji wymagamy jakości rozwiązań komercyjnych. Jest to psychologicznie uzasadnione, bo przyzwyczailiśmy się, że zgodnie z polskimi przepisami, odpłatne i darmowe udostępnianie usług w formie aplikacji odbywa

[1] Więcej na ten temat https://niebezpiecznik.pl/post/czy-zoom-jest-bezpieczny-czy-nie/

się na analogicznych zasadach - wymaga opracowania regulaminu ich udostępniania oraz zapewnienia odpowiedniego poziomu prywatności. Dotyczy to jednak firm, które mają siedzibę na terenie Unii Europejskiej lub państw Europejskiego Obszaru Gospodarczego. Wiele aplikacji jest udostępnianych przez firmy zagraniczne, zgodnie z przepisami zagranicznego prawa. Dlatego kluczowe jest zastanowienie się do czego chcemy wykorzystać ściąganą aplikację i przeczytać regulamin, który określa jak działa aplikacja oraz jakie są zasady zapewnienia prywatności i odpowiedzialność dostawcy rozwiązania.

Regulamin warto jednak przeczytać przed instalacją

Kto czyta regulaminy aplikacji? Zwykle prawnicy. Większość osób ściągając aplikację po prostu klika przycisk „akceptuję", żeby przejść do instalacji. W przypadku ZOOM kwestie dotyczące przekazywania danych do Facebooka nie były zawarte w regulaminie ani zawartej w nim polityce prywatności. Dlatego warto zastanowić się, czy nasze dane mogą być wykorzystane w większym zakresie niż podany i na ile może to stanowić problem. W ten sposób wracamy do fundamentalnej kwestii – jakimi danymi zasilamy aplikacje, których używamy. Mowa tutaj nie tylko o danych świadomie wprowadzanych do aplikacji – jak login, adres, telefon czy e-mail. Chodzi również o czytanie informacji o fizycznej lokalizacji naszego urządzenia, wyszukiwanych frazach czy stronach, na jakie wchodzimy.

RODO tworzy tylko ramy bezpieczeństwa

Zasady dotyczące ochrony danych osobowych obywateli UE dotyczą nie tylko firm, które mają siedzibę w jednym z państw członkowskich. RODO obowiązuje każdego, kto przetwarza dane Europejczyków. Inną kwestią jest, w jaki sposób dochodzić swoich praw z tym związanych od firm, które nie podlegają prawu UE. W przypadku ZOOM firma deklarowała, że jej zasady prywatności są zgodne z RODO. Wymóg taki wynika zresztą z art. 3 ust. 2 lit. a) RODO, to znaczy obowiązuje podmioty oferujące usługi obywatelom UE, nawet jeżeli odbywa się to nieodpłatnie. To znaczy, że zbieranie danych bez odpowiedniej informacji narusza obowiązki informacyjne wobec użytkowników wynikające z art. 13 RODO. Dodatkowo „wyciek" danych do Facebooka powinien był być zakwalifikowany jako incydent ochrony danych osobowych. Można się zastanawiać, komu ZOOM powinien był go zgłosić – biorąc pod uwagę zakres użytkowników można uznać, że do któregokolwiek organu ochrony danych osobowych w państwach swoich europejskich użytkowników (reszta powinna być skoordynowana przez organ wiodący wyznaczony zgodnie z RODO). Z pewnością informacje o wycieku powinny trafić do osób, których to dotyczyło, a sam ZOOM podjąć działania eliminujące problemy bezpieczeństwa. Co do tego ostatniego, jak widać po ostatnich doniesieniach – tak się nie stało.

Ustawienia domyślne trzeba personalizować

Część problemów związanych z logowaniem się na spotkania w ZOOM obcych osób wynikało z niewłaściwego ustawienia widoczności wydarzeń i zasad dostępu do nich. Użytkownicy nie mają wpływu na dopuszczalną długość haseł, jednak dobra znajomość wyświetlających się komunikatów i znajomość zasad działania aplikacji pozwala na ustalenie czy spotkanie jest nagrywane. Po ostatniej aktualizacji, możliwość reakcji na taką

sytuację ma być łatwiejsza. Brak zgody na określone przetwarzanie danych przez aplikację powinna być zawsze taka sama – wylogowanie się z sesji.

Używać czy nie używać?

W każdej sytuacji wskazany jest zdrowy rozsądek. Z aplikacji ZOOM nie powinno się korzystać do prowadzenia spotkań, na których poruszane są szczególnie wrażliwe kwestie czy wymieniane wrażliwe dane, których nie omawialibyśmy w kawiarni czy firmowym open space. Dotyczy to jednak również innych komunikatorów, których bezpieczeństwa nie zweryfikowaliśmy. W obecnej sytuacji wiele firm musiało wdrożyć szybkie rozwiązania, które z dnia na dzień pozwoliły na wdrożenie pracy zdalnej. Szybkie, czyli nie zawsze sprawdzone i bezpieczne. Dlatego najważniejsze to odpowiedzieć sobie na pytanie – jak chcemy wykorzystywać aplikacje, jakie dane mają być przesyłane, w jaki sposób (głosowo, na czacie, w plikach), na jakich urządzeniach będzie instalacja (do jakich innych danych można z uzyskać z niego dostęp). Bez względu na to jaką decyzję podejmiemy – powinniśmy to zrobić świadomie. Zwłaszcza, że za naruszenie bezpieczeństwa w aplikacjach, których używamy, odpowiadamy również my. W zakresie danych, które mieliśmy obowiązek chronić a wprowadziliśmy do aplikacji.

Autor: Monika Bogdał, radca prawny, kieruje specjalnością Nowe Technologie, Kancelaria Prawna Piszcz i Wspólnicy sp.k.