aut. Andrzej Kozłowski 21.09.2020

PRYWATNOŚĆ W CENTRUM UWAGI, CZYLI JAK STWORZYĆ BEZPIECZNĄ PLATFORMĘ DO WIDEOKONFERENCJI

„Temat cyberbezpieczeństwa platformy Webex to nie tylko kwestia funkcjonalności, jakie można włączyć lub wyłączyć na poziomie aplikacji, to jest kwestia spojrzenia na całościową politykę budowania systemu bezpieczeństwa" – mówi Artur Czerwiński, Dyrektor Techniczny Cisco. Ekspert wyjaśnia, jak Cisco przygotowało swoją platformę na pandemię oraz jakie wnioski wyciągnęło na przyszłość.

Jak pandemia wpłynęła na popularność usługi Cisco Webex? Czy firma była na to przygotowana?

Pandemia to wydarzenie niespodziewane i trudno się na nie przygotować. Szacujemy, że w okresie początkowym nastąpił gwałtowny wzrost liczby użytkowników, co najmniej trzykrotny w skali globalnej. W Polsce było to od 8 do 10 razy więcej osób w ciągu pierwszych tygodni. Ten skok był olbrzymi i przy takiej skali jest to zawsze ogromne wyzwanie zarówno z perspektywy technologicznej, jak i organizacyjnej. Na szczęście platforma Webex wykorzystywana jest w biznesie od 15 lat, więc jest dojrzała i w krótkim czasie została dostosowana do zwiększonych potrzeb. Oczywiście przejście na pracę zdalną wyłącznie w oparciu o Webeksa było też wyzwaniem organizacyjnym dla pracowników. Cisco od lat wspiera możliwość pracy zdalnej i dzięki temu przestawienie praktycznie całej organizacji na taki tryb działania nie stanowiło większego problemu. Przykładem może być nasze centrum wsparcia technicznego w Krakowie, gdzie pracuje ok. 2000 osób, które w ciągu dwóch dni całkowicie przestawiły się na model pracy zdalnej, realizując wszystkie zadania bez żadnych przerw.

Jednak wielu naszych klientów, którzy nie wprowadzili wcześniej takiego modelu pracy, m.in. placówki edukacyjne, musiało zmierzyć się z ograniczeniami technologicznymi. I tu Cisco przyszło z pomocą. Byliśmy jedną z pierwszych firm, która zaproponowała czasowe udostępnienie nieodpłatnych licencji na krytyczne w takiej sytuacji produkty, czyli właśnie na platformę Webex oraz produkty pozwalające na bezpieczny zdalny dostęp. Między innymi to było powodem, że zainteresowanie naszą platformą było ogromne i trudno też było dokładnie przewidzieć, jakie będzie obciążenie systemu.

Jakie niedogodności początkowo Państwo napotkali?

Początkowo obserwowaliśmy okresowe problemy z jakością połączeń, w szczególności przy komunikacji wideo wysokiej rozdzielczości. Natomiast te problemy pojawiały się jedynie przez pewien czas i nie wpłynęły na stabilność platformy. Warto podkreślić, że Webex to największa globalna komunikacyjna usługa chmurowa, wspierana przed kilkadziesiąt centrów danych na całym świecie, która obsługuje ponad 500 milionów użytkowników. W tym gorącym okresie Cisco podjęło działania na wielką skalę, które spowodowały, że w ekstremalnie krótkim czasie rozbudowano centra danych obsługujące Webeksa, zwiększając kilkukrotnie wydajność całego systemu. Dzięki temu udało się

utrzymać ciągłość pracy usługi, jednocześnie obsługując ten niespotykany ruch i olbrzymie obciążenie, które pojawiło się w rekordowo krótkim czasie.

Jakie rozwiązania bezpieczeństwa Cisco zaimplementowało w ramach swojej platformy, żeby uniknąć problemów, jakie miała konkurencja?

Temat cyberbezpieczeństwa platformy Webex to nie tylko kwestia funkcjonalności, jakie można włączyć lub wyłączyć na poziomie aplikacji, ale całościowego podejścia do architektury systemu, w ramach której bezpieczeństwo jest zawsze na pierwszym miejscu. Począwszy od polityki tworzenia bezpiecznego oprogramowania, przez wbudowane w platformę funkcje bezpieczeństwa, aż po mechanizmy ochrony danych osobowych. Takie podejście wynika wprost z naszej strategii, którą wyraził prezes Cisco Chuck Robbins. Powiedział, że prawo do prywatności jest podstawowym prawem człowieka i żeby je zapewnić, musimy mieć nie tylko mechanizmy ochrony, ale również transparentną komunikację o tym, jak bezpieczeństwo jest realizowane. Z tym założeniem wiąże się nasza polityka budowy platformy Webex, stworzenia usługi i jednocześnie informowania o tym, jak ona jest realizowana, bo jest to potrzebne użytkownikom z perspektywy wielu różnych procesów.

Platforma Webex od samego początku była stworzona z myślą o biznesie, czyli musiała spełniać wymagania np. podmiotów podlegających różnorodnym regulacjom. Musieliśmy zbudować rozwiązanie spełniające wysokie wymagania dotyczące m.in. prywatności danych. Cisco posiada dedykowany portal, który bardzo precyzyjnie informuje, w jaki sposób realizowana jest polityka prywatności danych platformy Webex: co dzieje się z danymi, kto ma do nich dostęp, jak długo i gdzie są przechowywane. To proces transparentnej komunikacji i w związku z tym użytkownik czy firma mają pełną świadomość, co dzieje się z ich danymi i jak są one wykorzystywane.

Inny obszar to bezpieczne tworzenie oprogramowania, które zawiera wrażliwe dane użytkowników i klientów biznesowych. Cisco nie dopuszcza do sytuacji, w których znaleźli się nasi konkurenci, gdzie pierwszym testerem cyberbezpieczeństwa był tak naprawdę klient. Mamy proces tworzenia oprogramowania Cisco Secure Development Life Cycle zawierający ok. 200 punktów kontrolnych dotyczących cyberbezpieczeństwa, które są zawsze sprawdzane i testowane, zanim produkt zostanie udostępniony na rynku. Przeprowadzamy również wewnętrzne testy podatności aplikacji, zanim ją udostępnimy klientom, żeby uniknąć kompromitujących wpadek. Mamy też transparentną politykę komunikacji. Jeśli pojawi się jakaś usterka, która zostanie wykryta, Cisco PSIRT (Product Security Incident Response Team) natychmiast informuje o tym fakcie klientów i partnerów. Pozwala to budować świadomość i umożliwia odpowiednią reakcję.

W jaki sposób można kontrolować prawidłowy przebieg spotkania?

Platforma Webex posiada rozbudowane funkcje, które pozwalają na kontrolowanie spotkania i zarządzanie nim. Pozwalają one m.in. na to, żeby nie dopuścić do dołączenia do spotkania intruza albo przekazania przez jakąś osobę treści, która jest niepożądana czy wręcz szkodliwa. Dzięki temu byliśmy w stanie zapobiec sytuacjom, które miały miejsce w przypadku innych platform. Nasze mechanizmy kontroli wiążą możliwość uczestnictwa w spotkaniu z poprawną identyfikacją końcowego użytkownika.

Poza weryfikacją posiadania konta w platformie Webex mamy również możliwość kontroli uczestnictwa w spotkaniu poprzez integrację z systemami usług katalogowych, autentykacji czy systemami uwierzytelnienia wieloskładnikowego, np. Cisco Duo Security, z których korzystają firmy do weryfikacji pracowników. Posiadamy też szereg mechanizmów, które pozwalają na to, żeby spotkania wychodzące poza macierzystą organizację były bezpieczne.

Istnieje np. możliwość ustawienia różnych profili w Webeksie i zdefiniowania w ramach profilu

uprawnień użytkowników dołączających do spotkania. Przykładowo można ustawić pewien wzorzec spotkania, w którym użytkownicy mogą czatować, ale nie mogą współdzielić treści innego typu. Mogą też mieć po dołączeniu do spotkania wyłączony mikrofon, dopóki prowadzący nie włączy go dla wszystkich lub tylko wybranych uczestników.

Cisco Webex posiada bardzo ciekawą funkcję tzw. poczekalni, która powoduje, że świadomie możemy decydować, kogo wpuszczamy na spotkanie. Jest to działanie podobne do tego, kiedy w rzeczywistości decydujemy, kogo wpuszczamy do mieszkania, sprawdzając wcześniej np. przez wizjer, czy wiemy, z kim mamy do czynienia. Dzięki temu, jeśli ktoś próbuje dołączyć do spotkania Webex, a nie jest znany organizatorowi, to zostaje w poczekalni tak długo, aż gospodarz podejmie decyzję. Trwające już spotkanie można również zamknąć dla intruzów, którzy próbują dołączyć w trakcie bez wiedzy organizatora. Zamknięcie spotkania trochę przypomina zamknięcie pokoju na klucz. Można to zrobić zarówno bezpośrednio z poziomu gospodarza spotkania, ale również automatycznie, ustawiając zamknięcie np. po 5 minutach od rozpoczęcia. Webex informuje prowadzącego spotkanie, że ktoś do niego dołączył. Jeśli widzimy, że jest to osoba uwierzytelniona, nie ma żadnego problemu. W przypadku, kiedy mamy informacje o dołączeniu użytkownika, który figuruje jako gość, możemy zatrzymać dyskusję i zapytać, kto to jest. Jeśli to osoba niepożądana, gospodarz spotkania może ją po prostu usunąć. Te mechanizmy pozwalają na bardzo skuteczne kontrolowanie sytuacji zarówno przed spotkaniem, jak i w jego trakcie.

Jak wygląda kwestia szyfrowania na platformie?

Webex oferuje kompletne szyfrowanie zarówno transmisji związanej z samym zestawieniem wideokonferencji, jak i przekazu treści audio, wideo oraz materiałów współdzielonych. Są tu zastosowane bardzo zaawansowane mechanizmy szyfrowania, m.in. TLS 1.2 czy AES-256. Ponadto istnieje możliwość włączenia szyfrowania E2E, przy której klucze szyfrujące są generowane i dystrybuowane przez aplikację Webex Meetings działającą na stacji końcowej gospodarza spotkania.

W takiej sytuacji Cisco jako dostawca platformy nie ma możliwości wglądu w jakiekolwiek dane, ponieważ zarówno ruch, jak i dane są szyfrowane, a kontrola nad tym procesem znajduje się po stronie klienta.

O bezpieczeństwie rozwiązań Cisco świadczą również liczne certyfikaty wydane przez zewnętrzne podmioty. Cisco stara się przekazać klientom, że tam, gdzie korzystanie z systemów wideokonferencyjnych w ramach pracy zdalnej staje się podstawą komunikacji, czyli działania przedsiębiorstw, warto mieć rozwiązania, które są sprawdzone przez zewnętrznych ekspertów. Cisco Webex posiada m.in. certyfikaty ISO 27001, ISO 27017, SOC2 typ II (Service Organisation Control), GDPR oraz HIPPA. Mamy również certyfikaty amerykańskiej administracji FedRamp czy niemieckiej C5, które, jak wiadomo, przykładają wielką wagę do kwestii cyberbezpieczeństwa.

Jakie są największe zalety Cisco Webex i co odróżnia ten produkt od rozwiązań konkurencji?

Aż 95% firm z listy Fortune 500, czyli rankingu 500 największych amerykańskich przedsiębiorstw, używa Webeksa. To pewien wykładnik jakości i wiarygodności rozwiązania. Z perspektywy klienta biznesowego, niezależnie, czy mówimy o małym, czy dużym podmiocie, największą zaletą jest wszechstronność, która pozwala na swobodny wybór najlepszego dla danej organizacji sposobu pracy. W ostatnim okresie często widzimy firmy pracujące w modelu hybrydowym, gdzie sporo pracowników pracuje zdalnie, a część z nich powróciła już do biur. Pojawia się potrzeba skomunikowania. W biurach infrastruktura jest inna i mamy do dyspozycji np. sale wideokonferencyjne czy dedykowane terminale wideo. Pamiętajmy, że są też osoby pracujące zdalnie, które mają dostęp tylko do laptopa czy smartfona. Dla nas bardzo ważne jest, żeby użytkownicy w łatwy sposób korzystali z technologii

niezależnie od miejsca i urządzenia, które mają do dyspozycji i żeby nie musieli martwić się o sposób organizacji takich spotkań. Wbrew pozorom nie jest to rzecz prosta, w szczególności, gdy nie ma dobrej integracji oprogramowania z elementami infrastruktury oraz innymi aplikacjami, np. kalendarzem firmowym. Akurat w przypadku tego typu aplikacji Webex ma wygodnie działającą integrację z MS Outlook i G-Suite, co pozwala na ograniczenie całej złożoności uruchomienia wideokonferencji do naciśnięcia jednego guzika widzianego w zaproszeniu e-mailowym lub na terminalu wideo. Cisco posiada ten przywilej, że jest zarówno dostawcą Webeksa, który działa na każdym typie urządzeń mobilnych, oraz producentem elementów infrastruktury jak terminale wideo. Pozwala to na wprowadzenie dodatkowych, unikalnych możliwości, które szczególnie w okresie pandemii mogą stanowić nie tylko udogodnienie, ale też służyć podniesieniu bezpieczeństwa pracowników.

Dzięki zastosowaniu algorytmów sztucznej inteligencji, do uruchomienia wideokonferencji Webex za pomocą terminala wideo można używać komend głosowych bez konieczności dotykania panelu sterującego. Co ciekawe można aktywnie monitorować liczbę osób w pomieszczeniu z systemem wideokonferencyjnym. Pozwala on np. informować o przekroczeniu liczby osób akceptowalnej dla konkretnej sali w kontekście zachowania odpowiedniego dystansu.

Inną z zalet Webeksa jest koncepcja prywatnych pokojów spotkań w chmurze, czyli tworzenie wirtualnych gabinetów i pokojów konferencyjnych. Wirtualne pokoje są bezpośrednią analogią do osobistego gabinetu w świecie rzeczywistym i stanowią ułatwienie dla osób mających problem z korzystaniem z technologii. Pokoje mogą być na stałe przypisane do użytkownika, zawsze aktywne i łatwe do identyfikacji, bo np. skojarzone z adresem email. Dzięki temu współpracownicy wiedzą od razu, jaki jest adres danego pokoju, kto w nim przebywa i jak się do niego dostać. W związku z tym nie potrzeba budowy skomplikowanej filozofii zaproszeń i mechanizmu administracyjnego, który dla wielu użytkowników bywa kłopotliwy. Wystarczy wysłać informację, np. spotykamy się w moim pokoju o konkretnej godzinie.

Istnieje też możliwość skorzystania z unikalnego narzędzia Webex Control Hub dającego dodatkowe możliwości administracyjno-analityczne. Dzięki niemu można budować profile spotkań, definiować parametry bezpieczeństwa, zarządzać infrastrukturą. Control Hub pozwala również np. na zdalne wymazanie danych na utraconych smartfonach bez konieczności inwestowania w dedykowany system typu MDM (Mobile Device Management).

Dodatkowo za pomocą Control Huba można analizować sytuację dotyczącą jakości połączeń dla danego spotkania i użytkownika. Diagnostyka pozwala na dość szybkie wykrycie źródła problemu, czy jest nim stacja końcowa użytkownika, wydajność sieci, czy też styk organizacji z internetem. Nasi konkurenci nie są w stanie dokonać tak pogłębionej analityki bez dodatkowych narzędzi.

W początkowym okresie pandemii mieliśmy sytuację, że pracownicy jednego z naszych klientów w Polsce musieli się przełączyć na pracę zdalną i wyszło, że są problemy z jakością komunikacji. Początkowo wydawało się, że to problem z systemem Webex, ale po analizie przeprowadzonej przy pomocy Control Huba okazało się, że ten konkretny klient miał problem ze zbyt małą przepustowością połączenia z internetem i wina leżała nie po stronie aplikacji, tylko możliwości obsłużenia zwiększonego ruchu na poziomie sieci. Wykrycie tego bez Control Huba nie byłoby takie proste.

Jakie wnioski Cisco wyciągnęło dla swojej platformy i jaki jest kierunek rozwoju na przyszłość?

Kluczowa jest wszechstronność platformy i stałe wprowadzanie ułatwień funkcjonalnych, połączone z ciągłym procesem podnoszenia jakości. Istotne też, żeby użytkownik mógł zrozumieć, jakie są jego potrzeby i potrafił wykorzystać to, co już dziś daje system. Przykładowo Webex jest najczęściej

kojarzony z systemem wideokomunikacyjnym, lecz w ramach platformy dostępny jest też moduł Webex Teams, przeznaczony do współpracy grup roboczych, które potrzebują możliwości interakcji i współdzielenia zasobów nie tylko w czasie bezpośredniego spotkania. Następuje dynamiczny rozwój zastosowania algorytmów sztucznej inteligencji. Możliwe jest np. uzyskanie automatycznie tworzonej transkrypcji nagranego spotkania, którą można wykorzystać jako gotową notatkę czy dokumentację. Warto również wspomnieć o aspekcie cyberbezpieczeństwa związanego ze współdzieleniem materiałów nie tylko wewnątrz firmy, ale również w ramach współpracy z klientami i partnerami. W tym zakresie istotna jest możliwość ograniczenia możliwości utraty wrażliwych danych w trakcie takiej komunikacji, co Webex realizuje przez nowe integracje z systemami kategorii DLP (Data Loss Prevention). Warto nadmienić, że do pewnego stopnia kierunki rozwoju Webeksa wyznaczają bezpośrednio użytkownicy, bo dzięki otwartym API możliwe jest włączenie platformy Webex do istniejących w firmie systemów. Przykładem może być integracja Webeksa z dziennikiem elektronicznym, która automatyzuje proces komunikacji nauczyciel – uczeń, ale w taki sposób, że to dziennik jest aplikacją, w której prowadzi się cały proces.