Cyberdefence 24

aut. Artykuł Promocyjny 08.07.2020

BEZPIECZEŃSTWO TELEKONFERENCJI W ERZE PANDEMII

Tysiące pracowników musiało przejść na tryb pracy zdalnej w zasadzie w mgnieniu oka. Kiedyś przyzwyczajeni do spotkań w salach konferencyjnych, dziś muszą pozostać w domach i spotykać się w przestrzeni wirtualnej. Nie zawsze są to łatwe i komfortowe warunki pracy. W całym zamieszaniu spowodowanym nietypową sytuacją nie można zapominać o bezpieczeństwie home office.

Cyberprzestępcy starają się wykorzystywać masowe przejście użytkowników na pracę zdalną. Koncentrują się między innymi na próbach wyłudzania dostępu do aplikacji czy danych użytkowników, głównie po to, aby w ten sposób wejść w posiadanie danych firmowych. Do tego celu stosują złośliwe domeny, phishing czy wzmożony trend wyszukiwania informacji związanych z wirusem COVID-19 i np. prowadzą do dezinformacji użytkowników.

Przestępcy „złowią" Cię na koronawirusa. Phishing w czasie pandemii

Mając na uwadze bezpieczeństwo zdalnych kadr, Cisco na bieżąco analizuje i śledzi złośliwe kampanie dotyczące koronawirusa i niepokojące alerty związane z tą tematyką. Do 19 lutego, klienci biznesowi firmy wysłali 562 144 zapytań do 8 080 unikalnych domen zawierających słowa kluczowe związane z tematyką pandemii, zachorowań, etc. Z kolei do 19 marca firma odnotowała 1 907% wzrost liczby zapytań, czyli 11 287 190 zapytań na 47 059 domenach zawierających słowa skorelowane z obecną sytuacją na świecie spowodowaną wirusem. 4% z tych 47 000 domen zostało zablokowanych jako złośliwe strony.

Eksperci ds. cyberbezpieczeństwa zrzeszeni w Cisco Talos zaobserwowali znaczny wzrost aktywności na polu ataków phishingowych, wykorzystujących sytuację związaną z koronawirusem w takich kategoriach, jak wypuszczanie do sieci złośliwego oprogramowania (tzw. malware). Na popularności zyskują również, niestety, kampanie phishingowe, czyli te polegające na podszywaniu się pod konkretne osoby lub instytucje, które jako „przynętę' wykorzystują materiały o tematyce COVID-19. Niestety na porządku dziennym są również coraz częściej ataki na organizacje, które prowadzą badania oraz aktywną działalność na rzecz walki ze skutkami wirusa. Jednocześnie zespół odpowiadający za usługę Cisco Umbrella analizuje obecnie ponad 180 miliardów zapytań internetowych dziennie, chroniąc użytkowników przed potencjalnie zainfekowanymi miejscami w sieci. Eksperci firmy obserwują złośliwe działania skierowane do klientów firmy, nakierowane m.in. na zdobywanie dostępu i uprawnień do ich kont w różnych programach i usługach lub do pobierania złośliwego oprogramowania.

„Eksperci Cisco badają wszystkie obszary, które mogą być narażone na ataki cyberprzestępców w nowej biznesowej normalności. Ostatnie miesiące pokazały jak ważne jest bezpieczeństwo aplikacji i systemów wykorzystywanych w biznesie, w szczególności do współpracy. Dzięki zaangażowaniu i umiejętnościom naszych zespołów ds. bezpieczeństwa, udało nam się w czasie pandemii, kiedy aktywność cyberprzestępców była wyjątkowo duża, ochronić miliony użytkowników" - mówi

Przemysław Kania, Dyrektor Generalny Cisco w Polsce.

Jako największe przedsiębiorstwo zajmujące się cyberbezpieczeństwem na świecie, Cisco ochroniło miliony użytkowników, którzy przeszli na tryb pracy zdalnej. Firma rozszerzyła program darmowych licencji na kluczowe technologie, które służą do ochrony pracowników wykonujących swoje zadania z domowego zacisza:

- Bezpieczeństwo warstw DNS od Cisco Umbrella. Cisco Umbrella odnotowało dwukrotny wzrost liczby zapytań o darmowe licencje w porównaniu do typowej tygodniowej średniej;
- Uwierzytelnienie wieloskładnikowe od Duo Security. Odnotowano dwucyfrowy wzrost rejestracji w stosunku do standardowej liczby w podobnym okresie. Całkowita miesięczna liczba wzrosła z 600 milionów w lutym do 800 milionów w kwietniu, głównie z powodu przejścia na tryb pracy zdalnej.
- Bezpieczny dostęp do sieci za pomocą Cisco AnyConnect (VPN). W kwietniu, odnotowano wzrost liczby dziennych zalogowań o 180% w porównaniu do standardowego ruchu obserwowanego w lutym. Co istotne, liczba użytkowników stale się utrzymuje na podwyższonym poziomie.

Bezpieczne telekonferencje

Masowe przechodzenie na pracę zdalną spowodowało, że gwałtowanie wzrosło zainteresowanie platformami do obsługi wideokonferencji. Rozwiązania do współpracy, takie jak Cisco Webex są obecnie podstawowym narzędziem dla biznesu, szkół, administracji publicznej i służby zdrowia, pozwalającym na pozostanie w kontakcie, realizację zadań i obowiązków. Stały się one również celem ataków cyberprzestępców, którzy wiedzą, że teraz, częściej niż kiedyś, użytkownicy udostępniają za ich pośrednictwem dane wrażliwe. Najbardziej znanym rodzajem ataków było tzw. "zoom bombing" polegający na dołączaniu do trwającej wideokonferencji niepowołanych uczestników, którzy bardzo często przeszkadzają w jej prowadzeniu np. głośną muzyką, wyzwiskami bądź wyświetlaniem na ekranach urządzeń wykorzystywanych do komunikacji niepożądanych treści (np. pornograficznych).

Mając na uwadze potencjalne zagrożenia związane z telekonferencjami, należy szczególnie dbać o bieżące aktualizacje, gdyż niezałatane podatności mogą stanowić furtkę dla nieuczciwych użytkowników sieci. Z kolei producenci, wiedząc o większym zainteresowaniu ich usługami, powinni transparentnie informować o wszelkich lukach w rozwiązaniach do współpracy.

„W obecnych, niepewnych czasach rekomendujemy korzystanie z narzędzi, w których bezpieczeństwo jest funkcją podstawową, wbudowaną w rozwiązanie i nie wymaga skomplikowanej konfiguracji. W przypadku wielu dostępnych na rynku rozwiązań często nie jest to normą. Funkcjonalność i wygoda nie mogą być jedynym kryterium wyboru rozwiązania do współpracy. Muszą im towarzyszyć funkcje zapewniające bezpieczeństwo. Warto również sprawdzić, gdzie są przechowywane dane wysyłane za pośrednictwem wykorzystywanej przez nas aplikacji” – mówi Przemysław Kania, Dyrektor Generalny Cisco w Polsce.

Dlatego warto korzystać ze sprawdzonych rozwiązań, takich jak Cisco Webex, które:

- automatycznie przypisuje spotkaniom i ich uczestnikom indywidualne identyfikatory i hasła,
- zapewnia całościowe szyfrowanie danych przesyłanych między uczestnikami,
- blokuje nieuprawniony dostęp osób trzecich,
- przygotowuje transkrypcję rozmów w oparciu o wewnętrzną aplikację Cisco (Voicea), dzięki czemu nie są one przechowywane na zewnętrznych serwerach.

Nawet najbezpieczniejsze narzędzia do współpracy nie uchronią organizacji przed cyberatakiem, jeżeli użytkownicy również nie przyłożą szczególnej uwagi do kwestii bezpieczeństwa. Eksperci Cisco

opracowali 4 rekomendacje, które pozwolą nie paść ofiarą cyberataku:

1. **Wyłącz wszystkie narzędzia i funkcje, których nie używasz** – gdy skończysz określoną czynność pamiętaj, aby wyłączyć: mikrofon, aparat, udostępnianie ekranu czy udostępnianie plików. Pracując w domu czujemy się swobodniej niż w biurze, dlatego warto zasłonić kamerę w komputerze. Pamiętaj, że niektóre aplikacje do wideokonferencji automatycznie włączają wideo, gdy tylko dołączysz do rozmowy lub gdy zezwalasz gospodarzom na włączenie funkcji wideo u uczestników.
2. **Przygotuj się do udostępniania ekranu** – jeżeli zamierzasz udostępniać ekran podczas telekonferencji, wyłącz powiadomienia na pulpicie i upewnij się, że tapeta i inne okna nadają się, aby zaprezentować je uczestnikom wirtualnego spotkania. Dotyczy to w szczególności urządzeń prywatnych, wykorzystywanych do celów służbowych.
3. **Zastanów się, w jaki sposób zapewniony jest dostęp do wirtualnych spotkań**– najlepiej będzie, jeśli Twoje narzędzia do pracy zdalnej będą zintegrowane z rozwiązaniami bezpieczeństwa oferującymi uwierzytelnianie wieloskładnikowe (np. Cisco Duo Security) czy ochronę urządzeń końcowych (np. Cisco Advanced Malware Protection for Endpoints), które zapewnią dodatkową warstwę zabezpieczenia firmowych zasobów, niezależnie od tego z jakiego miejsca łączą się z nimi ich użytkownicy.
4. **Wymagaj zgody gospodarza spotkania na dodawanie gości i udostępnianie nagrań** – mimo, że telekonferencje od dawna są standardem w wielu organizacjach, teraz odbywa się ich więcej niż kiedykolwiek. Świadczy o tym fakt, że tylko w marcu, odbyło się 14 miliardów minut spotkań za pośrednictwem platformy Cisco Webex (ponad dwa razy więcej niż w lutym, gdy pandemia koronawirusa nie objęła jeszcze tak dużej części świata). W natłoku spotkań można się pogubić kto dokładnie bierze w nich udział. Na takie sytuacje czekają cyberprzestępcy, którzy mogą stać się nieproszonym gościem. Dlatego zawsze należy mieć kontrolę nad tym kto uczestniczy w spotkaniu i jakie ma uprawnienia np. czy może odsłuchać jego przebieg, jeżeli było ono nagrywane.

Materiał powstał we współpracy z Cisco.

Patrz więcej:

Sign up free, it's quick

Praca z domu

Dbamy o łączność i komunikację w czasie epidemii COVID-19

Cisco Capital