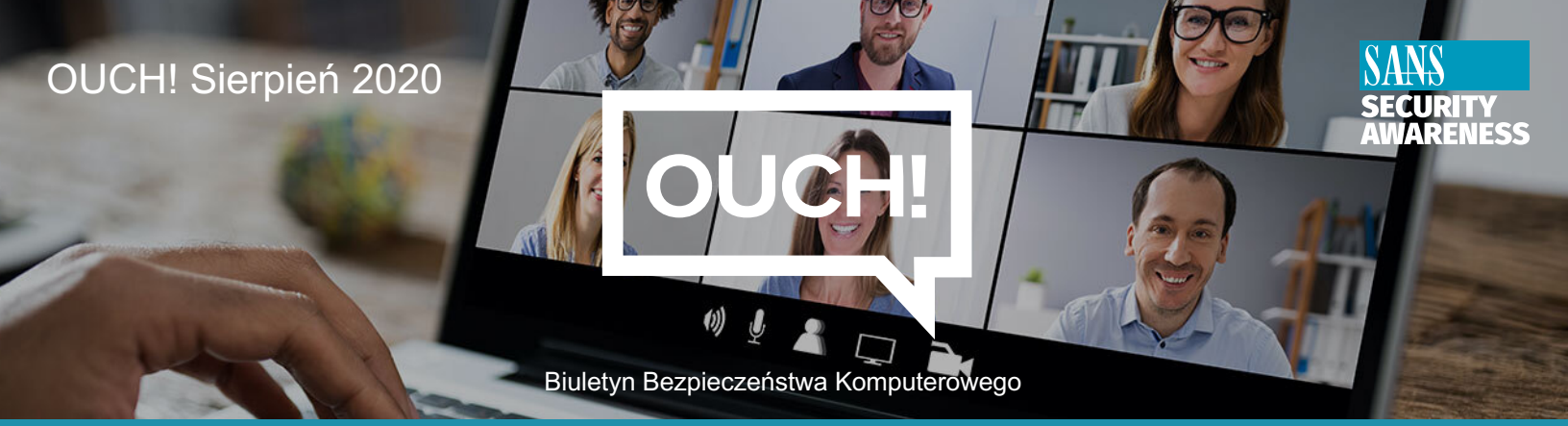
OUCH! Sierpień 2020



Bezpieczeństwo wideokonferencji

Czym są wideokonferencje?

Coraz więcej osób ma możliwość pracy zdalnej z domu. Do kontaktu ze współpracownikami, przełożonymi często używamy programów do wideokonferencji takich jak Zoom, Slack czy Microsoft Teams. Wideokonferencje nie służą jedynie do kontaktów stricte biznesowych. Tej technologii można również używać do łączenia się z przyjaciółmi lub do nauki. Bez znaczenia w jakim celu korzystasz z programów do wideokonferencji, poniżej przedstawimy kluczowe kroki, które zobrazują Ci jak korzystać z tej technologii w sposób maksymalnie bezpieczny.

Udział w wideokonferencji

Jeśli masz zamiar brać udział w wideokonferencji powinieneś zapoznać się z pięcioma kluczowymi zasadami.

1. **Zaktualizuj aplikację**: Upewnij się, że zawsze korzystasz z najnowszej wersji oprogramowania do wideokonferencji. Świeże i zaktualizowane oprogramowanie jest kluczowe do zachowania bezpieczeństwa połączenia. Włącz opcję automatycznych aktualizacji, gdyż tylko wtedy masz pewność, że aktualizacja zostanie zainstalowana tuż po jej opublikowaniu.
2. **Konfiguracja ustawień audio/wideo**: W ustawieniach włącz opcję, która wyciszy mikrofon oraz wyłączy kamerę za każdym razem kiedy dołączasz do spotkania. Aby zapewnić większe bezpieczeństwo, rozważ zasłonięcie obiektywu kamery internetowej w momencie kiedy z niej nie korzystasz. Pamiętaj, że podczas wideokonferencji każdy może zobaczyć co robisz, nawet kiedy nic nie mówisz.
3. **Sprawdź co jest za Tobą**: Jeśli zdecydujesz się na włączenie kamery internetowej, skontroluj co znajduje się za Tobą. Sprawdź czy nie znajdują się tam żadne osobiste ani wrażliwe przedmioty, których nie chcesz pokazywać wszystkim podczas połączenia. Niektóre programy do obsługi wideokonferencji pozwalają na rozmycie lub ustawienie wirtualnego tła, dzięki czemu inni uczestnicy konferencji nie widzą tego, co znajduje się z tyłu.
4. **Nie dziel się zaproszeniem**: Można powiedzieć, że link do zaproszenia jest twoim osobistym biletem wstępu na spotkanie. Nawet jeśli znany Ci współpracownik potrzebuje tego linku, o wiele prościej i bezpieczniej będzie poprosić organizatora konferencji o indywidualne zaproszenie.
5. **Nie nagrywaj**: Nie rób zrzutów ekranu ani nie nagrywaj połączenia konferencyjnego bez odpowiedniego pozwolenia. Poprzez niesubordynację możesz przypadkowo udostępnić bardzo wrażliwe informacje jeśli te zrzuty ekranu lub nagrania zostaną upublicznione.

Prowadzenie wideokonferencji

Jeśli przyjdzie Ci organizować w przyszłości wideokonferencję, weź pod uwagę niżej wymienione kroki.

1. **Wymagaj hasła**: Aby zapewnić bezpieczeństwo, prywatność oraz kontrolować dostęp do wideokonferencji, ustaw hasło dostępowe. W ten sposób tylko osoby posiadające hasło będą mogły dołączyć do spotkania.
2. **Sprawdź uczestników spotkania**: Weryfikuj ludzi uczestniczących w konferencji. Jeśli jest ktoś, kogo nie znasz lub masz trudności ze zidentyfikowaniem, niech ta osoba potwierdzi swoją tożsamość. Jeśli ktoś zakłóca spokój i jest nieuprzejmy, usuń taką osobę z wideokonferencji. Zadbaj o dobrą atmosferę spotkania. Niektóre programy do obsługi wideokonferencji umożliwiają zablokowanie spotkania po rozpoczęciu, tak aby nikt więcej nie mógł do niego dołączyć bez zgody. Istnieje również rozwiązanie polegające na wstępnym umieszczaniu uczestników w wirtualnej poczekalni, tak aby zweryfikować ich tożsamość.
3. **Poinformuj o nagrywaniu**: Jeśli zamierzasz nagrywać spotkanie (i masz na to pozwolenia), pamiętaj aby poinformować wszystkich o tym.
4. **Udostępnianie ekranu**: Jeśli zechcesz udostępniać ekran komputera, pamiętaj aby najpierw zamknąć wszystkie inne aplikacje i ukryć poufne pliki z pulpitu. Wyłącz również wszelkie powiadomienia z aplikacji. Pomoże to uniknąć przypadkowego upublicznienia poufnych lub wstydliwych informacji podczas udostępniania ekranu komputera. Zamiast udostępniać cały ekran komputera, zastanów się nad udostępnianiem tylko tej aplikacji, którą chcesz pokazać.

Technologie te są interesującym narzędziem i na wiele sposobów reprezentują przyszłość tego, w jaki sposób będziemy pracować, współpracować oraz komunikować się z innymi. Wyżej przedstawione wskazówki pozwolą Ci w pełni korzystać z technologii wideokonferencji w sposób maksymalnie bezpieczny.

Redaktor gościnny

Lodrina Cherne jest głównym rzecznikiem ds. bezpieczeństwa w firmie Cybereason, chroniąc wszystkich ludzi i informacje w dzisiejszym otwartym i zinternetyzowanym świecie. Lodrina przekazuje wiedzę o Windows forensics w instytucie SANS oraz współtworzy blog ThisWeekin4n6. Na Twitterze można znaleźć ją jako @hexplates.

Źródła

Tworzenie haseł w prostszy sposób: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Menedżer haseł: https://www.sans.org/security-awareness-training/resources/password-managers-0

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz.