Warszawa, 31 lipca 2019 r.

**Ostrożnie z hotspotami.**

**Jak dbać o bezpieczeństwo danych w podróży**

**W delegacji czy podczas urlopu coraz mniejszym problemem jest znalezienie miejsc z bezpłatnym dostępem do internetu. Otwarte sieci Wi-Fi, szczególnie za granicą, są dla podróżnych „oknem na świat”. To wygodna alternatywa dla często kosztownej transmisji danych w roamingu. Korzystając z hotspotu na lotnisku, w restauracji czy hotelu można sporo zaoszczędzić, ale też stracić. Urządzenia podłączone do publicznej sieci są łatwym celem dla cyberprzestępców. Jak się przed tym zabezpieczyć?**

Zagraniczne wojaże – zarówno te wakacyjne, jak i służbowe – stają się coraz łatwiejsze za sprawą nowych technologii. Obecnie trudno sobie wyobrazić podróż bez telefonu, który służy już nie tylko do kontaktu z bliskimi czy współpracownikami. Urządzenia mobilne pozwalają dokonać rezerwacji noclegu, zaplanować dojazd na lotnisko lub sprawdzić prognozę pogody w dowolnym miejscu na świecie. Dodatkowo coraz częściej przejmują funkcje służbowych komputerów, umożliwiając wygodne wysyłanie maili i przeglądanie dokumentów na lotnisku czy w pociągu.

*Z doświadczenia wiem, że wielogodzinne oczekiwanie na lot sprzyja pracy. W dodatku najpopularniejsze lotniska przesiadkowe dysponują specjalnymi strefami z dostępem do internetu, a nawet salami konferencyjnymi. Dla osób, które spędzają dużo czasu w drodze to dobra okazja, aby nadrobić zaległości. W moim przypadku często to jedyny moment, by sprawdzić maile, zanim na dłuższą chwilę stracę łączność ze światem. W odległych zakątkach świata uzyskanie dostępu do sieci jest dość problematyczne, dlatego staram się najpilniejsze sprawy związane z firmą załatwić jeszcze w trakcie podróży. Zwykle moje biuro jest tam, gdzie służbowy komputer i telefon*  – **powiedział Jarosław Nowak, podróżnik, przedsiębiorca i właściciel EcoGlobe Travel**.

**Ryzyko utraty danych**

Jak wynika z badania „Smartfon w firmie. Bezpieczeństwo danych w telefonach służbowych” 51% pracowników korzysta ze służbowych urządzeń elektronicznych w przestrzeni publicznej. Większość z nich (74%) ma świadomość związanych z tym zagrożeń wynikających m.in. z logowania się do otwartych sieci Wi-Fi[[1]](#footnote-1). Darmowy dostęp do internetu w galeriach handlowych, kawiarniach lub na lotniskach może być dla użytkowników źródłem wielu problemów. Złośliwe oprogramowanie czy wyłudzenie danych (phishing) to tylko przykłady pułapek zastawianych przez cyberprzestępców. Działania hakerów są poważnym, ale nie jednym w tej sytuacji niebezpieczeństwem dla służbowych urządzeń mobilnych. W zatłoczonych miejscach nie trudno też o zgubienie lub kradzież telefonu bądź tabletu, z czym spotkało się odpowiednio 41% i 35% respondentów.

**Bez odpowiedniej ochrony ani rusz**

Urządzenia mobilne są obecnie podstawowym narzędziem pracy oraz nośnikiem ważnych danych firmowych, dlatego warto zapewnić im odpowiednią ochronę. Systematyczne aktualizacje systemu operacyjnego, instalowanie oprogramowania antywirusowego i zapór sieciowych oraz zabezpieczanie urządzeń hasłem pozwalają zminimalizować ryzyko. Warto zaufać też sprawdzonym rozwiązaniom.

*Najwyższy poziom bezpieczeństwa zapewniają mi zaawansowane systemy oraz funkcje ochrony danych i prywatności mojego telefonu. Stworzony przez BlackBerry program DTEK sprawdza wszystkie zainstalowane aplikacje i informuje mnie o wykrytych zagrożeniach, np. ich nieuprawnionym dostępie do kontaktów, lokalizacji, aparatu lub mikrofonu albo wysyłaniu podejrzanych wiadomość tekstowych. W podróży bardzo przydaje mi się też funkcja Privacy Shade chroniąca poufne informacje przed ciekawością osób postronnych. Aplikacja zaciemnia wyświetlacz, zostawiając podgląd jedynie wybranej części ekranu. Dzięki temu mogę przeglądać nawet poufne dokumenty bez obaw, że ktoś zagląda mi przez ramię* – **dodał Jarosław Nowak.**

W podróży lepiej też unikać łączenia się z otwartymi sieciami Wi-Fi. Szczególnie w przypadku serwisów wymagających logowania, bezpieczniej jest skorzystać z własnego pakietu transmisji danych. Na wypadek sytuacji awaryjnej warto zadbać o to, by telefony miały mobilne łącze VPN oraz oprogramowanie chroniące prywatność podczas korzystania z niezaufanej sieci. Warto zadbać też o szyfrowanie danych, dzięki czemu nawet jeśli smartfon trafi w niepowołane ręce, informacje zapisane w pamięci będą bezpieczne. Bez znajomości hasła na nic zda się nawet podłączenie urządzenia do komputera i skopiowanie danych, bo tak czy inaczej, będą nieczytelne.

\*\*\*

**O badaniu**

Badanie „Smartfon w firmie. Bezpieczeństwo danych w telefonach służbowych” zostało przeprowadzone na przełomie kwietnia i maja 2019 r. metodą CAWI na reprezentatywnej próbie 1002 aktywnych zawodowo użytkowników służbowych telefonów komórkowych przez SW Research na zlecenie Cyfrowego Centrum Serwisowego S.A., dystrybutora telefonów BlackBerry. Celem badania było sprawdzenie świadomości firm w zakresie ochrony danych cyfrowych, bezpieczeństwa użytkowania urządzeń elektronicznych, w tym służbowych telefonów komórkowych oraz związanych z tym zagrożeń.

**Cyfrowe Centrum Serwisowe S.A.** prowadzi działalność z zakresu dystrybucji i serwisu urządzeń mobilnych. Najważniejszym celem realizowanej przez spółkę strategii jest świadczenie najwyższej jakości usług w oparciu o własne wieloletnie doświadczenie oraz zaufanie klientów.

Firma rozpoczęła działalność w 2000 roku w okresie dynamicznego rozwoju polskiego rynku telefonii komórkowej oraz rosnącego zapotrzebowania na urządzenia mobilne i obsługę serwisową. W ciągu wielu lat zdobyła zaufanie klientów i partnerów biznesowych oraz uzyskała silną pozycję eksperta na rynku telekomunikacyjnym.

Jako jedna z pierwszych firm w Polsce CCS otrzymało status autoryzowanego serwisu sprzętu mobilnego, a dziś należy do grona najlepszych centrów serwisowych na świecie. Ścisła współpraca z wiodącymi producentami pozwoliła również na stworzenie bogatej i konkurencyjnej oferty w zakresie sprzedaży produktów.

Dzięki wysoko wykwalifikowanej kadrze oraz stosowanym rozwiązaniom informatycznym i logistycznym Cyfrowe Centrum Serwisowe zapewnia profesjonalną, wygodną, a także bezpieczną obsługę w obszarze dystrybucji oraz serwisu urządzeń mobilnych.

1. Badanie „Smartfon w firmie. Bezpieczeństwo danych w telefonach służbowych” przeprowadzone na przełomie kwietnia i maja 2019 r. przez SW Research na zlecenie Cyfrowego Centrum Serwisowego S.A., dystrybutora telefonów BlackBerry. [↑](#footnote-ref-1)