aut. Tomasz Fastyn 18.07.2016

PODCZAS WYJAZDU CHROŃ SWOJE URZĄDZENIE TAK SAMO JAK SWOJE ZDROWIE

Portal darkreading przygotował dla swoich czytelników kilka prostych porad jak uchronić i zabezpieczyć się na czas masowych imprez, takich jak np. igrzyska olimpijskie w Brazylii w tym roku. W przypadku chorób zakaźnych stosujemy odpowiednie szczepionki czy leki np. na malarie będąc w krajach egzotycznych. Warto zastosować takie dobre praktyki także wobec naszych urządzeń mobilnych, które zabieramy ze sobą.

Szczególnie narażonymi osobami na cyberataki, podsłuchiwanie czy nawet zwykłą kradzież mienia są osoby prowadzące aktywną działalność biznesową nawet podczas wypoczynku. Najłatwiejszym rozwiązaniem wydawało by się jest zostawienie wszelkich urządzeń elektrofonicznych w depozycie bankowym jednak kto dziś może obyć się bez telefonu podczas codziennego dnia, a co dopiero podczas wyjazdu. Samo zostawienie urządzenia w pokoju hotelowym, nawet wyposażonym w teoretycznie bezpieczny zamek elektroniczny wydaję się nie stanowić przeszkody dla hakerów. Według darkreading chwalili się oni już od jakiegoś czasu, że włamanie do sejfu z elektronicznym zamkiem nie stanowi wielkiej przeszkody. Najbezpieczniej w takim razie nosić ze sobą urządzenia, które są dla nas cenne lub posiadają istotne informacje o nas.

Nie możemy zapominać także o tym, że ktoś może nas podsłuchiwać, nawet pokój hotelowy może mieć w standardzie mikrofon podsłuchujący wszystkie nasze rozmowy. Dlatego wstrzymajmy się od przekazywania informacji wrażliwych poprzez telefon, szczególnie hasła dostępu czy ważnych informacji handlowych. Jeżeli musimy podać komuś dane dostęp do naszego konta, ponieważ jesteśmy odcięci dostępu do komputera to najlepiej wysłać je za pomocą bezpiecznego szyfrowanego kanału.

Jak czytamy dalej na stronie darkreading podczas tak dużych masowych imprez pojawi się wiele kampanii phishingowych wymierzonych w niczego nieświadomych turystów. Warto zwracać uwagę na to co ściągamy, z jakich aplikacji korzystamy oraz gdzie szukamy informacji dot. imprezy. Warto w tym miejscu zwrócić się tubylców o informacje jakie aplikacje czy strony są oficjalnymi kanałami komunikacji, tak aby uniknąć bycia na celowniku oszustów.

Jednak sam problem z cyberbezpieczeństwem może pojawić się zanim wylądujemy na lotnisku w pobliżu Rio. Chodzi m.in. o kupowanie biletów czy wynajmowanie nocy w hoteli. Niestety w tym miejscu musimy być ostrożni, najlepiej sprawdzić dokładnie gdzie i z jakiego źródła kupujemy bilet. Już od jakiegoś czasu, według Trend Micro pojawiają się fałszywe strony oferujące bilety w atrakcyjnych cenach. Niektóre z nich, oprócz oferowania biletu, którego nie ma zbierają dane, które później mogą posłużyć do wyczyszczenia naszego konta bankowego.

Inny pomysłem na ochronę swojej prywatności oraz urządzeń, które są dla nas cenne jest kupienie taniego telefonu wraz z lokalną kartą sim. Taką kampania aktualnie działa z powodu nadchodzącej Olimpiady „Know the Risk; Rise Your Shield” przygotowanej przez amerykańskie Narodowe Centrum

Kontrwywiadu i Cyberbezpieczeństwa (NCSC). Rozwiązaniem może także być zabranie taniego telefonu ze sobą, ważne jednak, żeby był sformatowany fabrycznie, tak aby nie posiadał danych wrażliwych.

– Zainstaluj inną przeglądarkę na potrzeby podróży poza granice kraju w którym mieszkasz. Powinieneś także używać innej przeglądarki przy połączeniach z niezaufanymi sieciami WiFi czy hotspotami – radzi Shaun Murphy z Private Giant. Dobrym rozwiązaniem może okazać się także używanie trybu incognito czy szyfrowanej przeglądarki np. Tor. Rozwiązaniem, o którym wspomina darkreading jest także VPN. W tym miejscu można skorzystać z gotowych komercyjnych rozwiązań dostępnych na rynku lub wykorzystać domowy router jako urządzenie przekierowujące ruch sieciowy.

– Zwracaj uwagę na powiadomienia jakie pojawiają się na urządzeniu. Jeżeli urządzenie mówi, że połączenie jest niebezpieczne, to takie prawdopodobnie jest. Podobnie w przypadku korzystania z punktów dostępowych, jeżeli zostaniesz poproszony o instalacje oprogramowania, natychmiast rozłącz się z sieci i nie instaluj żadnego oprogramowania. Zwykle takie aplikacje mogą być złośliwe i spowodować znaczne szkody w urządzeni z którego korzystasz – podkreśla Shaun Murphy.

Ostatnie o czym wspomina portal darkreading jest sprawdzenie po powrocie, czy nie złapaliśmy podczas naszego wyjazdu żadnego wirusa, nie chcemy wnosić zarażonego urządzenia do naszej bezpiecznej sieci. Warto zmienić hasła, jakich używaliśmy poza granicami, nie zaszkodzi przeskanować urządzeń odpowiednim antywirusem, warto także rozważyć przywrócenie do ustawień fabrycznych.

Czytaj też: Euro 2016 pożywką dla hakerów - raport