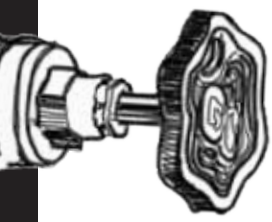
5/2016

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 5/2016

Czy ten gość na pewno do ciebie?

Wielkie zaskoczenie przeżyli co poniektórzy właściciele inteligentnych dzwonków do drzwi Ring. Urządzenie to, w zasadzie kamera wyposażona w moduł wifi, komunikuje się z siecią domową i za pośrednictwem aplikacji przekazuje zdalny obraz sprzed drzwi na ekran komórki. Na skutek błędów w integracji baz danych, niektórzy posiadacze dzwonka mogli oglądać nagrania spod mieszkań lub domów zupełnie obcych ludzi. To nie pierwsze kłopoty Ringa. Luka wykryta kilka miesięcy temu pozwalała na przejęcie domowej sieci wifi przez obce osoby. A producent chwali się, że Ring oferuje „nowy poziom bezpieczeństwa". Po tej serii wpadek dzwonek chyba już definitywnie stracił przydomek „inteligentnego". Jeśli więc posiadasz Ringa i na podglądzie widzisz stojącą pod drzwiami piękną kobietę lub przystojnego mężczyznę nie biegnij otwierać drzwi, bo bardzo prawdopodobne, że to gość do sąsiada.[1]

Lekcja z Facebooka

Małżeństwo Martinez spod Nowego Jorku padło ofiarą nietypowego ataku scamerów. Mąż odebrał telefon i w słuchawce usłyszał krzyczącego mężczyznę, który twierdził, że żona pana Martineza potrąciła na parkingu przed szpitalem jego kuzyna i chciała zbiec z miejsca wypadku. „Jesteśmy dealerami narkotyków z Bronxu i nie mamy ubezpieczenia, chcemy, żebyś zapłacił za koszty leczenia" – krzyczał mężczyzna. Szantażował Martineza, że złapali jego żonę i jeśli wkrótce nie dostaną pieniędzy, to pobiją ją. W tle słychać było histerycznie płaczącą kobietę. Rzecz w tym, że żona Martineza faktycznie przebywała w tym czasie w szpitalu odwiedzając swoją matkę. Kochający mąż długo nie wahał się – przelał rzekomym porywaczom 1300 dolarów. Po 2 godzinach okazało się, że to oszustwo – niczego nieświadoma kobieta wróciła cała i zdrowa do domu. Okazało się, że wcześniej zameldowała się na Facebooku, komentując swoją wizytę w szpitalu. Cóż, za nieroztropność żony w tym przypadku największą lekcję offline z zachowań online dostał mąż. Pozostaje liczyć na to, że i sama kobieta wyciągnie z niej wnioski. [2]

Drogi autograf

Dlaczego podczas płacenia kartą kredytową nigdy nie powinieneś podpisywać rachunku, jeśli wcześniej wprowadziłeś numer PIN?

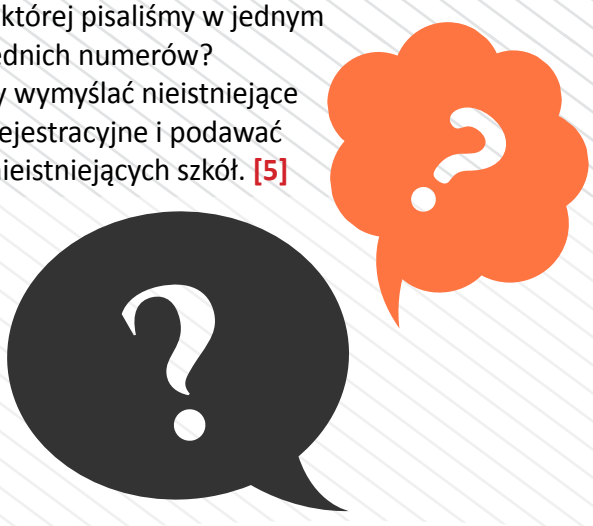
Przed taką praktyką ostrzega profesor Basie Von Solms, dyrektor Centrum Cyberbezpieczeństwa z Uniwersytetu w Johannesburgu. Często zdarza się, że mimo wcześniejszego użycia PINu do autoryzacji transakcji, sprzedawcy proszą o dodatkowe podpisanie paragonu. „Tak nie powinno być. Regulacje jasno mówią, że jeśli używasz PINu, nie musisz nic podpisywać".
Ekspert przestrzega, że przestępcy mogą wykorzystać złożony podpis, aby ustalić imię i nazwisko klienta, które w połączeniu z numerem karty kredytowej i jej datą ważności pozwala w łatwy sposób wykraść pieniądze.
Poproszony więc o podpis, odmów grzecznie, tłumacząc, że autografów nie rozdajesz. To przecież może być twój najdroższy autograf w życiu. [3]

Podróżni na nasłuchu

Operator systemu transportu w New Jersey wprowadził na niektórych liniach pociągów, dodatkowo obok monitoringu wideo, również monitoring audio.
Naturalnie na reakcję obrońców prywatności nie trzeba było długo czekać. Władze zapewniając o poszanowaniu prywatności pasażerów, tłumaczą swoją decyzję względami ich bezpieczeństwa i przypominają o groźbie ataków terrorystycznych.
Jednak szczegółowej odpowiedzi na pytanie w jaki sposób dane audio są przechowywane, jak długo i kto ma do nich dostęp nie udzielają. „Jest prawo, które to reguluje, a my działamy zgodnie z nim" - ucinają.
Obrońców prywatności do tego pomysłu nikt nie przekona. „Gdy zadzwoni do ciebie lekarz, dziecko albo małżonek i udasz się do odosobnionej części pociągu, aby nikt cię nie słyszał, nie spodziewasz się, że możesz być podsłuchiwany" – mówi prawnik Ed Barocas, wskazując, że terroryzm jest w tej sprawie tylko tematem zastępczym.
My zastanawiamy się ile razem par oczu i uszu by potrzeba, aby tego typu monitoring mógł być faktycznie skuteczny?
Chyba jednak bardziej chodzi tu o pociąg do podsłuchiwania. [4]

Niebezpieczne pytania bezpieczeństwa

Pewna Amerykanka miała problemy z wypłatą gotówki z bankomatu, zadzwoniła więc do swojego banku wyjaśnić sprawę. „Dowiedziałam się, że muszę odpowiedzieć na trzy pytania bezpieczeństwa. Poległam na wszystkich trzech" – opowiada.
Okazało się, że jej konto bankowe przejęli hakerzy wyprowadzając z niego 2800 dolarów. Podający się za nią scamer wcześniej telefonicznie podał operatorowi poprawnie wszystkie odpowiedzi i zmienił pytania bezpieczeństwa. Hakerzy byli w stanie udzielić informacji odnośnie szkoły, do której właścicielka konta chodziła, numerów blach jej samochodu, a nawet banku, w którym miała kredyt.
Kobieta zgłosiła sprawę do banku i odzyskała pieniądze, ale zachodzi w głowę jak do tego doszło. Tymczasem eksperci ds. bezpieczeństwa podkreślają, że takie informacje przestępcy mogą łatwo kupić od hakerów, którzy włamali się do przeróżnych baz danych.
Wiele odpowiedzi da się też wyciągnąć z mediów społecznościowych.
Czyli wychodzi na to, że pytania bezpieczeństwa tak naprawdę żadnego bezpieczeństwa nie dają.
A może to dobry pomysł na rozszerzenie biznesu dla 11-latki, zajmującej się ręcznym generowaniem haseł, o której pisaliśmy w jednym z poprzednich numerów?
Mogłaby wymyślać nieistniejące tablice rejestracyjne i podawać adresy nieistniejących szkół. [5]



FUNDACJA bezpieczna cyberprzestrzeń

Strzelająca emotikonka

Ciekawą sprawą zajmował się ostatnio francuski sąd. Po rozpadzie związku młody mężczyzna wysłał swojej byłej dziewczynie smsa z emotikoną - pistoletem. Następnie nękał ją kolejnymi wiadomościami, do tego stopnia, że przerażona nieletnia ofiara bała się sama wychodzić z domu.
Mimo, że obrońca chłopaka podważał, aby samo wysłanie emotikonki mogło mieć na dziewczynę aż tak traumatyczny wpływ, a we francuskim prawodawstwie naturalnie brak zapisów dotyczących emotikonek, to sąd znalazł na mężczyznę paragraf. Uznał, że wysłanie obrazka z bronią podpada pod artykuł 222-17 francuskiego kodeksu karnego, który odnosi się do gróźb śmiertelnych.
W efekcie chłopaka skazano na trzy miesiące więzienia, w zawieszeniu na sześć. Dodatkowo musi zapłacić ofierze 1000 euro odszkodowania.
To pierwszy tego typu wyrok we Francji. Jeśli francuski sąd traktuje emotikony tak poważnie, to ciekawe czy są jakieś, które pozwoliłyby chłopakowi zrehabilitować się i wcześniej wyjść na wolność? [6]

[1] http://tinyurl.com/zms7nje
[2] http://tinyurl.com/juzwzlp
[3] http://tinyurl.com/hexz7hq
[4] http://tinyurl.com/jkjdd87
[5] http://tinyurl.com/zctpbdn
[6] http://tinyurl.com/hddu3g7

Kolejne numery można śledzić również na serwisie społecznościowym LinkedIn

CALL FOR SPEAKERS!

Jeśli możesz wzbogacić agendę SCS 2016 i masz ciekawą historię do przedstawienia, prześlij swoją propozycję!
Sprawdź jakich prezentacji szukamy?
www.securitycasestudy.pl/call-for-papers

Wśród prelegentów na tegorocznej konferencji SCS będziemy gościli Mikko Hypponena z F-Secure oraz Johna Martleya - twórcę słynnego serwisu Shodan. Chcesz dołączyć – prześlij swoje zgłoszenie!

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

www: https://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo