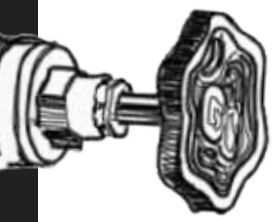
11/2014

FUNDACJA bezpieczna cyberprzestrzeń



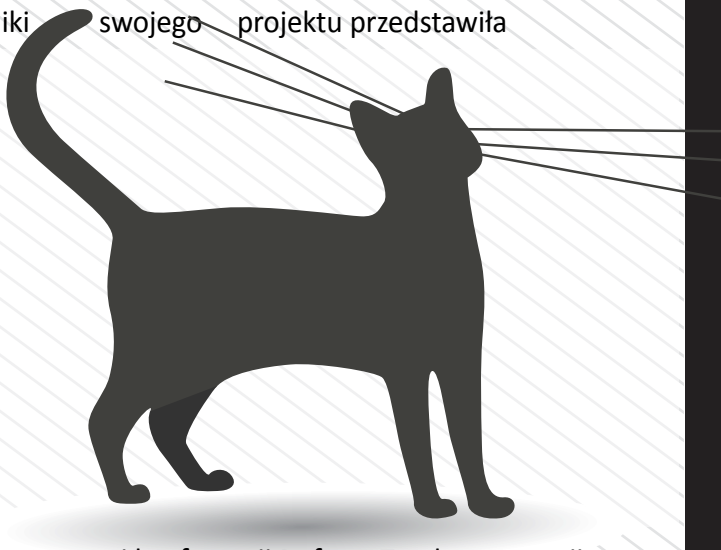
zawór bezpieczeństwa 11/2014

Urządzenia kontroli pasażerów z domyślnymi hasłami

Lotniska to miejsca, w których najbardziej aktywnie wprowadza się ograniczenia ze względu na bezpieczeństwo. Szkoda, że nie dotyczą one tych, którzy pilnują ich przestrzegania. Billy Rios przeprowadził badania, z których wynika, że w urządzeniach stosowanych do kontroli pasażerów na lotniskach, bardzo często stosowane są domyślne konta i hasła. Niektóre z nich są dostępne online co już jest największym poziomem zaniedbania. Wcześniej Rios wykazał słabe strony w urządzaniach skanujących bagaże. Szczególnie ryzykowny jest dostęp do wszystkich tych urządzeń z sieci Internet. Może się to skończyć penetracja całej sieci i urządzeń stosowanych na lotnisku. Nie trzeba „odlotowych" pomysłów aby z tym prostym problemem sobie poradzić. Administratorom lotniska podpowiadamy, że zmiana domyślnego hasła jest procesem podobnym do rezygnacji z przydzielania wszystkim pasażerom samolotu miejsca 1A.[1]

Kot Coco zbadał bezpieczeństwo sieci Wi-Fi

Projekty typu „wardriving" są już doskonale znane czytelnikom ZB. Występują najróżniejsze odmiany tych projektów, sieci Wi-Fi można wyszukiwać jeżdżąc samochodem, ale nie tylko. Można też to robić pieszo, byli też tacy, którzy uruchamiali projekty rowerowe. Na zupełnie nowy pomysł wpadła Gane Bransfield. Do projektu pozyskała kota swojego dziadka - syjamczyka o imieniu Coco. Przygotowała ona dla kota specjalną opaskę, która zawierała kartę Wi-Fi, moduł GPS i baterię. Zestaw ten (koszt zestawu poniżej 100 $) pozwolił na zmapowanie sieci bezprzewodowych na terenie przechadzek Coco. Wyniki swojego projektu przedstawiła



na tegorocznej konferencji Defcon. Tytuł prezentacji był niezwykle wymowny – „How To Weaponize Your Pets" („Jak uzbroić swoje zwierzaki domowe"). Kot w czasie projektu „odnalazł" wiele niezabezpieczonych sieci Wi-Fi, a całe przedsięwzięcie miało charakter uświadamiający i miało być dobrą zabawą. W ciągu godziny Coco odnalazł 23 sieci WiFi z czego ponad 1/3 była niezabezpieczona w ogóle lub bardzo slabo - tzn. korzystała z prostego do złamania algorytmu szyfrowania WEP. Kot też chyba był zadowolony z projektu - wrócił z łowów z jedną myszą, która ofiarował oczywiście swojemu panu. Pewnie mysz zakłócała pomiary. [2]

FUNDACJA bezpieczna cyberprzestrzeń

Hakowanie świateł ulicznych jest niestety dość łatwe

Do takiej właśnie smutnej konkluzji doszli naukowcy z Uniwersytetu w Michigan. Żadna zaawansowana wiedza nie jest do tego potrzebna, a najważniejsze akcesoria to laptop i odpowiedni odbiornik radiowy. System posiada trzy fundamentalne wady, a każda z nich jest praktycznie dyskwalifikująca jeśli chodzi o bezpieczeństwo. Te wady to: brak szyfrowania transmisji radiowej, używanie domyślnych haseł administracyjnych i dostępność portów serwisowych. Praktycznie wszyscy, którzy są w stanie odbierać transmisję o częstotliwości 5,8 GHz mają dostęp do systemu, gdyż ten ruch nie jest szyfrowany. Co więcej przesyłanie pakietów danych nie wymagało uwierzytelnienia. Wszystkie te wady sprawiały, że system jest nieodporny na większość ataków. Możliwe jest wydłużanie i skracanie czasu świecenia świateł, czy też uruchamianie zielonego albo czerwonego światła na danym kierunku przejazdu. Możliwy jest też atak typu DDoS, który może spowodować kompletny jego paraliż. Oby ten paraliż objawiał się czerwonym, a nie zielonym, światłem dla wszystkich nadjeżdżających. Krótko mówiąc jeśli widzicie w mieście samochód, który jakoś nie ma potrzeby zatrzymywania się na żadnym skrzyżowaniu bo zawsze ma zielone światło, to nie wykluczone, że w środku zasiada haker zmieniający światła na klawiaturze swojego laptopa.[3]

Cyberprzestępcy tweetami kierują ruchem lotniczym

Samolot linii lotniczych American Airlines - lot AA362 został zawrócony z trasy z Dallas do San Diego, po tym jak cyberprzestępcy poinformowali na Twiterze, że na jego pokładzie znajduje się ładunek wybuchowy. Samolotem podróżował szef Sony Online Entertainment - John Smedley. Serwis firmy Sony tego samego dnia (24/08/2014) był zaatakowany atakiem DDoS. Autorami tweeta „radzącego" aby dokładnie sprawdzić samolot była grupa „Lizard Squad", dokładnie ta sama która zaatakowała Sony. Incydent był poważny. Samolot musiał lądować kilkaset mil przed planowanym miejscem lądowania a pasażerowie byli z niego bezpiecznie ewakuowani. Pozostaje mieć nadzieje, że członkowie „Lizard Squad" szybko wylądują w celach więziennych i ten lot będzie przebiegał bez zbędnych zakłóceń. [4]

„Five finger discount" dla klientów Vibram

"Five finger discount" w języku angielskim oznacza zniżkę w wysokości 100%, tyle że po skorzystaniu z niej można skończyć za kratkami. Krótko mówiąc chodzi o sklepową kradzież z wykorzystaniem „pięciu palców". Podobnie można by nazwać atak na klientów marki Vibram, która to znana jest z produkcji tzw. „naturalnego" obuwia do biegania, a naturalność polega na tym, że buty posiadają właśnie pięć palców. Dobra okazja do gry słów, którą wykorzystał Dave Lewis z serwisu CSO Online. Opisał on wyciek danych klientów wspomnianej marki. Chodzi o numery kart kredytowych. Głównym powodem była bardzo słabo zabezpieczona platforma firmy hostingowej,

FUNDACJA bezpieczna cyberprzestrzeń

gdzie znajdował się serwis. Vibram już zmienia platformę, a klienci pewnie będą musieli zmienić swoje karty kredytowe. Niestety ofiar nie da się policzyć na palcach jednej nogi. [5]

Pan myszka sprzedaje dolary

Znany badacz ciemnych rewirów internetu, Brian Krebs widział już wiele przedmiotów i usług sprzedawanych na internetowym czarnym rynku. Niemniej jednak jedno z ostatnich jego znalezisk zaskoczyło jego samego. Niejaki Mr Mouse (w wolnym tłumaczeniu - Pan Myszka) oferował w nielegalnym serwisie podrobione banknoty dolarowe. Co prawda banknoty nie są do wykorzystania w automatach, które zazwyczaj sprawdzają występowanie tzw. „magnetycznego atramentu", ale większość innych testów wypada dla nich pozytywnie. Na przykład posiadają znaki wodne i nie są do zidentyfikowania poprzez test „flamastrem". Na sprzedaż wystawione zostały banknoty 20, 50 i 100 dolarowe. Pan Myszka nie będzie zapewne łatwy do ujęcia, ponieważ bardzo dba o bezpieczeństwo - informuje lojalnie: „ktokolwiek, kto pochodzi z „nikąd" i nie ma nazwy użytkownika formum - nie będzie obsłużony". Adres mailowy Pana Myszki jest z Niemiec dlaczego więc nie Herr Maus?[6]

[1] http://tinyurl.com/n3kbvnr
[2] http://tinyurl.com/k6du4fz
[3] http://tinyurl.com/q85l3lm
[4] http://tinyurl.com/nu5tzgh
[5] http://tinyurl.com/oxrjcj5
[6] http://tinyurl.com/k5w6xte

Kolejne nr można śledzić również na serwisie społecznościowym LinkedIn

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