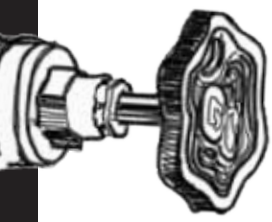
3/2017

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 3/2017

Piwne NIE-bezpieczeństwo

Ręczna pompa do piwa to urządzenie niezwykle szanowane w tradycyjnych pubach, szczycących się wyjątkowym smakiem serwowanego piwa. Czy może mieć coś wspólnego z cyberbezpieczeństwem? Przypadek pewnego mężczyzny pokazuje, że tak. Zapragnął on mieć taką pompę u siebie w domu i zamówił ją przez internet. Ta historia zahacza jednak o cyberbezpieczeństwo dopiero w momencie, gdy klient otworzył paczkę. Sprzedawca napracował się, aby dobrze przygotować przedmiot do wysyłki: pompa była zabezpieczona papierowymi ścinkami... rodem z biurowej niszczarki. Już na pierwszy rzut oka było widać, że nie najlepszej sprawności. Wśród dokumentów pociętych na grube paski łatwo było dostrzec wyciągi bankowe, notatki służbowe, czeki, tabele z wynikami. Jednym słowem – niezła gratka dla cyberprzestępców lub specjalistów od socjotechniki, którzy chcieliby kogoś poszantażować celem zdobycia wrażliwych informacji.

Jak widać w dzisiejszych czasach trudno zaufać nawet niszczarce. Już pewnie rozlane piwo mogłoby dokonać skuteczniejszych zniszczeń. [1]

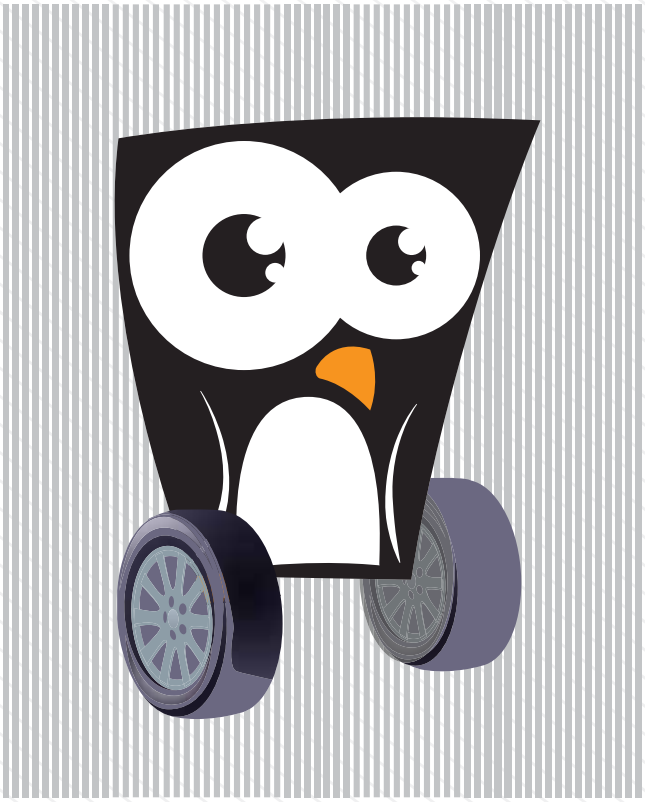
Podatek od robota

Czy robot, który zabrał Ci pracę powinien płacić podatki? Bill Gates nie ma wątpliwości. Automatyzacja w wielu dziedzinach jest już faktem, ale według założyciela Microsoftu podatek od robotów pozwoli choć trochę ją spowolnić i dofinansować inne dziedziny. Czy to nie zaskakujące stanowisko najbogatszego człowieka świata i techno-optymisty? Za pracowników firmy płaci się mnóstwo składek. Nie powinno więc być zaskoczenia opodatkowaniem pracujących robotów. Ostatecznie to i tak dla pracodawców oszczędność. W końcu robotom nie będą wypłacać pensji, robot nie pójdzie na urlop ani na zwolnienie chorobowe. Gates uważa, że dzięki opodatkowaniu maszyn można będzie dofinansować te sektory, w których

ludzie są niezbędni, np. szkolnictwo czy opiekę nad osobami starszymi i niepełnosprawnymi, przy której liczy się ludzka empatia. Niektóre firmy już kalkulują czy jednak nie taniej pozostać przy zatrudnianiu ludzi.
Nie trzeba ich naprawiać, serwisują się sami, a gdy coś zacznie poważnie szwankować łatwo delikwenta wymienić. [2]

Pingwiny inspiracją dla samochodów

Naukowcy nie raz odwoływali się do natury, aby znaleźć najlepsze rozwiązania dla swoich wynalazków. Tym razem zainspirowani zachowaniem pingwinów opracowali system testowania oprogramowania do samochodów. Twierdzą, że z pomocą w temacie przychodzą ich strategie łowieckie, wypracowane w ciągu tysięcy lat na trudnym terenie.Strategia przetrwania pingwinów polega na świetnej współpracy podczas połowu ryb, synchronizacji nurkowania i porozumiewaniu się głosem. Pozwala im ona uzyskać maksymalną ilość pożywienia przy minimalnym nakładzie energii. Jednym słowem idealna optymalizacja. Producenci współczesnych aut są pod coraz większą presją tworzenia interaktywnych rozwiązań, a odpowiedni software odgrywa w nich kluczową rolę.
W nowym systemie testowania chodzi o znalezienie optymalnego pomysłu, sprawdzenie integralności oprogramowania, poprawności przetwarzania danych oraz tego czy nie powoduje błędów, które mogłyby grozić wypadkiem.
A może przy okazji sprawdzić jak pingwiny sprawdziłyby się w roli kierowców takich inteligentnych aut? [3]



Nowe wcielenie legendy

Tej komórki zapewne nie trzeba Wam przedstawiać. Na początku lat 2000 była powszechnym obiektem pożądania; na emeryturę odeszła w 2005 roku. Nokia 3310, telefon-ikona z prawie niezniszczalną obudową i niezwykle wytrzymałą baterią, powraca. Jej odświeżoną wersję zaprezentowano na Mobile World Congress 2017 w Barcelonie. Nokia 3310 była najlepiej sprzedającym się telefonem świata. Łącznie rozeszło się około 126 milionów egzemplarzy. Na to, że miłość do marki nie wygasa liczy fiński producent HMD Global Oy, który chce wykorzystać nostalgię fanów i przyciągnąć sentymentalnych użytkowników, doceniających proste rozwiązania. Nowa-stara Nokia ma kosztować 59 euro. Odświeżona Nokia to kolorowy wyświetlacz, aparat, radio, odtwarzacz MP3 i 16mb wbudowanej pamięci. Bateria ma wytrzymać 22 godziny rozmów i miesiąc czuwania. No i najważniejsze: nie zapomniano o kultowej grze w węża.
W czasach smartfonów pociągnąć na jednym naładowaniu baterii długie godziny w węża to dopiero podróż w przeszłość. [4]

FUNDACJA bezpieczna cyberprzestrzeń

Robot, który „nie jest robotem”

I stało się. Robot zaśmiał się w twarz testowi CAPTCHA i kliknął w słynne zabezpieczenie „Nie jestem robotem”, które ma na celu ochronę danych przed maszynami i botami. Filmik dokumentujący jak ramię robota przesuwa kursor myszki touchpadem i naciska potwierdzenie zamieścił jeden z użytkowników na YouTube. Niewyraźny zlepek cyfr i liter irytował niejednego, który stanął przed wyzwaniem udowodnienia, że nie jest robotem. Całkiem niedawno Google wyszedł z pomysłem tzw. „Invisible ReCAPTCHA”, który nie będzie wymagał żadnego odznaczania checkboxa ani rozwiązywania graficznych łamigłówek i ma działać na stronach bez wiedzy użytkowników. Na upowszechnienie tego rozwiązania jeszcze jednak poczekamy. Jest więc nadzieja, że to nie ostateczny triumf robotów nad ludźmi. Swoją drogą ciekawe czy ów robot poradziłby sobie z odróżnieniem człowieka od robota, gdyby przyszło mu stanąć przed testem obrazkowym. To byłby prawdziwy test na człowieczeństwo ;-) [5]

Migotliwa sprawa

Nawet migająca na dysku twardym dioda może wyjawić z komputera poufne dane – donoszą eksperci z Izraela. Chodzi o sprzęt „offline”, nie podłączony do żadnej sieci i zupełnie odizolowany od świata zewnętrznego. W jaki sposób? Pierwszym krokiem cyberprzestępców jest zainfekowanie urządzenia malware, który potrafi odczytać dane przechowywane w pamięci komputera. Szkodliwe oprogramowanie jest trudne do wykrycia, a jego praca polega na sterowaniu diodą LED dysku twardego. Malware zamienia zera i jedynki na odpowiednie impulsy świetlne emitowane przez diodę. Aby mogło dojść do przechwycenia danych wystarczy, że niedaleko znajduje się kamerka, dron z kamerą albo po prostu kamera przemysłowa. Dane mogą być odczytane nawet z odległości 20 metrów. Podczas przekazywania danych dioda LED generuje impulsy świetlne tak szybko, że ludzkie oko nie wychwyci migania. Wydaje się, że dioda świeci się stale. To sposób na przejęcie danych dla wyjątkowo zdeterminowanych – najpierw trzeba włamać się do komputera, aby zainstalować malware, a potem jeszcze do kamery, aby móc oglądać mrugającą diodę. Czy teraz już oprócz kamerki trzeba będzie zaklejać również diodę taśmą? [6]

Kolejne numery biuletynu „Zawór Bezpieczeństwa” można również śledzić 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: https://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo