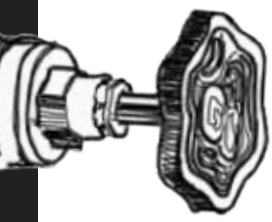
7/2014

FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 7/2014

Cyberprzestępcy „wypływają w morze”

Wygląda na to, że statki, stocznie i w ogóle transport morski a nawet morskie platformy wydobywcze stały się kolejnym obszarem zainteresowania cyberprzestępców.
Na 19 dni powstrzymali oni prawidłowe działanie jednej z platform wydobywczych. Cyberprzestępców zatrudniają też somalijscy piraci, którzy manipulują danymi nawigacyjnymi tak aby łatwiej dopaść swoje ofiary. Natomiast w porcie w Antwerpii cyberprzestępcy zaatakowali komputery obsługujące przeładunek kontenerów aby przejąć kontrolę nad tymi kontenerami, w których były przemycane narkotyki i usunąć ich dane z bazy. Jedna z brytyjskich firm ubezpieczeniowych oszacowała, że cyberataki mogą kosztować ten sektor ponad 2 mld $ do 2018 roku. Badania zrobione wśród firm zarządzających całą infrastrukturą transportu i gospodarki morskiej wskazują na to, że nie ma wśród nich zbyt dużego poruszenia i przejęcia się sprawą. Nie wykluczone w związku z tym, że czeka nas w niedalekiej przyszłości jakiś „Cyber-Titanic”. Oby zabrakło na nim pasażerów a orkiestra grała z mp3-ki. [1]

Warto walczyć z phisherami

Często walka z cyberprzestępcami jest bardzo frustrująca. Trudno się przed nimi obronić, jak się obronimy z jednej strony to przyłożą nam z drugiej a wymiar sprawiedliwości rzadko bywa naprawdę pomocny. W tym pesymistycznym obrazie pojawia się jednak światełko. Tym światełkiem są statystyki opublikowane przez APWG (Anty Phishing Working Group). Oczywiście chodzi o ataki typu phishing. Otóż okazuje się, że w II połowie 2013 roku blisko połowa z 681 zaatakowanych organizacji, t.j. tych których strony podrabiano i zwabiano ofiary, nie była wcześniej atakowana (chodzi o rok 2013). Co może wskazywać na to, że poziom obrony wielu organizacji jest już tak wysoki, że przestępcom przestaje się opłacać je atakować i przerzucają się na nowe cele. Atakowane sektory gospodarki online pozostają

te same - instytucje finansowe i rynek e-commerce. Atakujący też. Pamiętajcie - jeśli nie znacie dokładnie odpowiedzi na pytanie kto zaatakował w sieci - odpowiadajcie „Chińczycy!”. Najmniejsza szansa na pomyłkę. [2]

Prywatni detektywi łamali prywatność

Dużą skutecznością wykazywało się jedno z brytyjskich prywatnych biur detektywistycznych. Okazało się jednak, że jego sukcesy wynikały również z nielegalnego pozyskiwania danych osobowych. Biuro, które specjalizowało się w odzyskiwaniu długów, systematycznie oszukiwało firmy będące dostawcami mediów czy usług telekomunikacyjnych i wyciągało od nich dane swoich „ofiar”. W ciągu roku blisko 2 000 razy dopuścili się nielegalnego czynu, co zapewne należy interpretować jako pozyskanie tyluż rekordów. Ułatwianie sobie pracy kosztowało właścicieli biura około 70 000 funtów - taki był wyrok sądu. Przeliczając na nasze wyszło około 180 złotych za rekord. Nie tylko z tego powodu się nie opłaca. [3]

Czy cyberterroryści zaatakują muzea komputerowe?

Dość ekstremalny przykład zastoju technologii w infrastrukturze krytycznej w USA. Tamtejszy arsenał atomowy obsługiwany jest między innymi przez

urządzenia „karmione” 8-calowymi dyskietkami. Najmłodszym czytelnikom „Zaworu” przypominamy, że dyskietka to taki pen-drive. Ta o której piszemy miała, ... STOP - tzn. ma rozmiary i powierzchnię porównywalną z iPadem (tym dużym) i może pomieścić 1 MB (zakładamy, że chodzi o jej „najnowszą” wersję). Jedynym wytłumaczeniem jest to, że być może odpowiedzialni za bezpieczeństwo broni atomowej założyli strategię bezpieczeństwa opartą na tym, że najprawdopodobniej cyberterroryści, którzy by chcieli zainfekować urządzenia wirusem, będą mieli bardzo trudne zadanie w pozyskaniu 8-calowej dyskietki. Zapewne wszystkie muzeakomputerowe są już obstawione agentami CIA. [4]

Potrząśnij swoim telefonem a powiem ci kim jesteś

Zespół naukowców z USA (robimy wszystko, żeby nie pisać „amerykańscy naukowcy”) odkrył, że dane jakie generują sensory ruchu w niektórych smartfonach, zawierają dane pozwalające na identyfikację konkretnych telefonów. Coś w rodzaju odcisku palca aparatu telefonicznego. Chodzi o to, że jeżeli dane na temat ruchu telefonu (np: w aplikacji fitness, albo w grze na telefon) zostaną przekazane poza telefon, to jest możliwe skojarzenie wielu danych przesłanych w różnej sytuacji jako danych pochodzących z tego samego telefonu. Jak się łatwo domyślić takie bazy mogą tworzyć potężne narzędzie marketingowe

poprzez gromadzenie danych,które można skojarzyć z jednym profilem. Musi to szczególnie cieszyć wszystkich marketingowych speców, których smuciły coraz to większe restrykcje nakładane na „ciasteczka". Jak widać coraz trudniej chronić swoją prywatność. [5]

Ktoś ćwiczy wyłączanie lotnisk

Jeden z amerykańskich generałów powiedział kiedyś mniej więcej coś takiego: „Po co bombardować lotniska skoro można je wyłączyć." Wychodzi na to, że być może ktoś testuje tę strategię. Przynajmniej na lotniskach w południowej Kalifornii. Zaczęło się od tego, że lotnisko LAX (Los Angeles International) ogłosiło „ground stop" i było to z powodu „computer issues". Później problem powstał na jeszcze kilku innych lotniskach a sprawą zajmowała się FAA (Federal Aviation Administration). Na samym LAX 27 lotów zostało przekierowanych na inne lotniska, 27 innych było odwołanych i 212 opóźnionych. Awaria trwała ponad godzinę, a przywracanie normalnego ruchu znacznie dłużej. Naprawianie rozpoczęto od przyjmowania samolotów, te wylatujące pozostawały „uziemione". Nie wiadomo czy to oznacza, że problem z komputerem był na „wyjściu" a nie na „wejściu" (no może w przypadku lotniskowego komputera „wylocie" - „wlocie"). W każdym bądź razie uznano go za bardzo rzadki. Miejmy nadzieję, że były to ćwiczenia z „wyłączania lotniska". [6]

[1] http://tinyurl.com/m8q875m
[2] http://tinyurl.com/l46axfa
[3] http://tinyurl.com/m8k2cx2
[4] http://tinyurl.com/pvwgcdy
[5] http://tinyurl.com/l9xqdk9
[6] http://tinyurl.com/k8pvgka

Ministerstwo Administracji i Cyfryzacji wspólnie z Generalnym Inspektorem Ochrony Danych Osobowych oraz patronem konkursu - Fundacją Bezpieczna Cyberprzestrzeń zapraszają studentów do udziału w konkursie na aplikację mobilną przyjazną prywatności. więcej

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