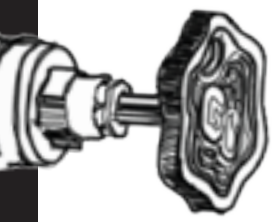
2/2013

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 2/2013

Po co aż tyle zasad bezpieczeństwa?

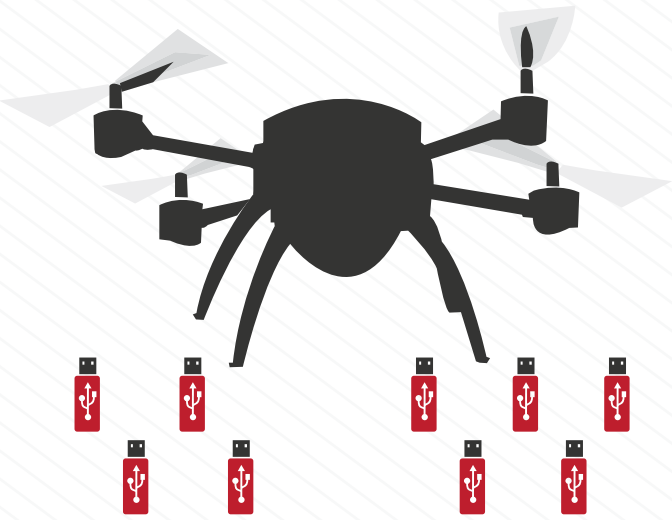
Holenderskie banki stworzyły zestaw pięciu zasad, które muszą spełniać klienci aby ubiegać się zwrot pieniędzy po ich utracie z konta. Hasła muszą być trzymane w tajemnicy, karta kredytowa nie może być pożyczana innym osobom, przepływy na koncie muszą być obserwowane, incydenty raportowane natychmiastowo a komputer do e-bankingu musi być zabezpieczony. I po co było tyle pisać - przecież wystarczy ostatni i nie będzie trzeba zwracać żadnych pieniędzy.[1]

Danych nie brakuje. Trzeba zacząć je wykorzystywać

ENISA wydała nowe opracowanie. Tym razem sprawa dotyczy dzielenia się informacjami na temat zagrożeń. Głównie przez CERT-y. W opracowaniu jest o barierach technicznych i prawnych, 100 proc. poparcia dla inicjatywy. Acz-kolwiek trzeba jeszcze wymyślić jak skutecznie te dane wykorzystywać. Z naszej perspektywy bowiem widać, że danych które można wykorzystać nie brakuje, tylko adresaci informacji o zagrożeniach w sieci niewiele z nimi robią.[2]

Nowy Stuxnet, a może dystyrbucja poprzez drony?

Nowa poważna cyber-koalicja na Bliskim Wschodzie. Izrael i Arabia Saudyjska wspólnie pracują nad nowym Stuxnetem przeciwko Iranowi. Ma być skuteczniejszy i bardziej destrukcyjny. Dodatkowo SA ma użyczyć IL terytorium do operacji z wykorzystaniem dronów. Kto wie - może w celu rozrzucania pen-drive'ów zawierających nowego Stuxneta.[3]



FUNDACJA bezpieczna cyberprzestrzeń

Kto będzie pilnował strażników?

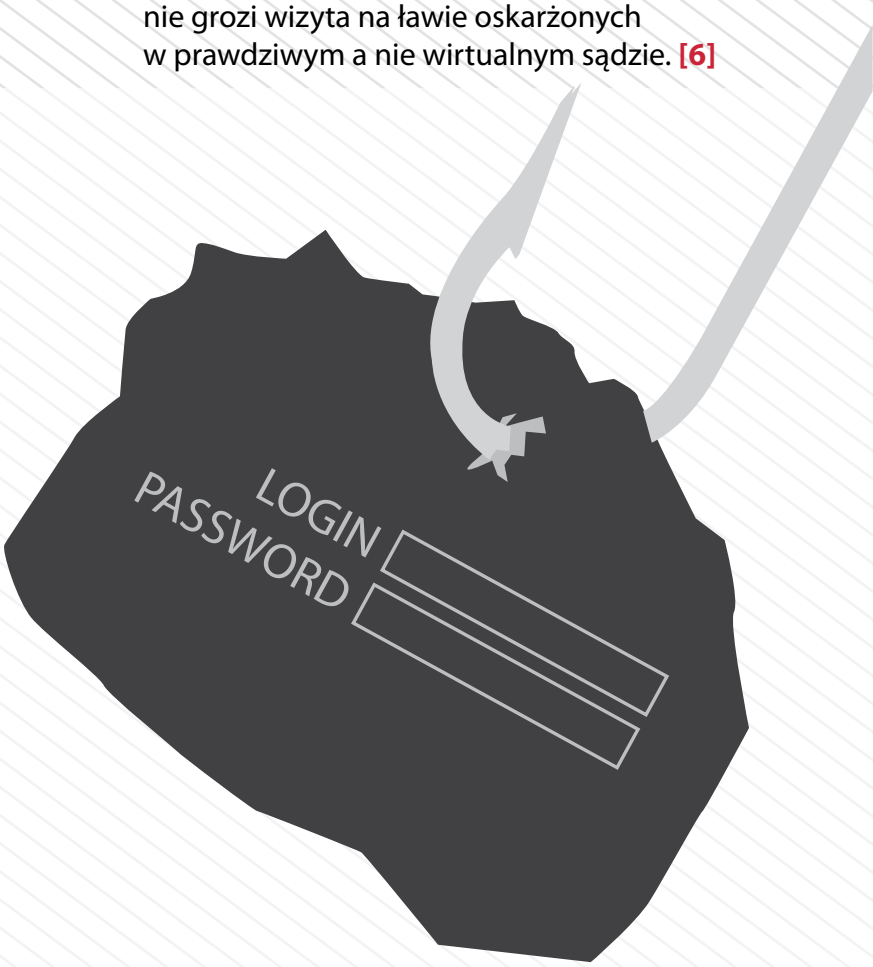
Gra online na pieniądze wymaga zaufania, wiary w to, że nie gramy z robotem, który bezwzględnie nas wypłucze z pieniędzy niczym rekiny finansowe drobnych spekulantów na giełdzie. Dlatego amerykański serwis ESEA przygotował dla grających oprogramowanie, które wykrywa oszustów internetowych. Wszystko było pięknie do czasu kiedy nie okazało się, że chroniący graczy software sam „prowadził wykopaliska" bitcoinów i oczywiście siebie jako oszusta nie wykrywał. „Quis custodiet ipsos custodes?"[4]

Chiński spear-phishing na pięciu MSZ krajów UE

"US_military_options_in_Syria" to tytuł załącznika na który dali się nabrać ministrowie spraw zagranicznych pięciu krajów UE. Rozsyłki phishingu dokonała chińska grupa hakerska "Ke3chang". Wszystko przy okazji szczytu G20 w 2012 w Meksyku. Aż się prosi informacja,w których to krajach ministrowie są podatni na takie ataki, możnaby było porównać te dane ze strategiami cyberbezpieczeństwa. Niestety nie wiadomo kim były ofiary. [5]

Nie zastrzel agenta w „Warcraft", nie obraź go w „Second Life"

Co najmniej od kilku lat amerykańscy i brytyjscy szpiedzy infiltrują GVE-y (Games and Virtual Environments). Są członkami hord Orków, lub "supermodelkami". Celem jest śledzenie terrorystów i innych wrogów, którzy masowo zaczęli wykorzystywać środowisko gier komputerowych do utajnionej komunikacji a nawet ćwiczeń bojowych. Podobno niektórzy z pilotów zamachu na WTC nigdy nie siedzieli za sterami prawdziwych samolotów a swoje umiejętności nabyli na symulatorze lotów Microsoft. Pozostaje nadzieja, że za strzelanie do agenta w grze internetowej lub obrażenie "supermodelki" nie grozi wizyta na ławie oskarżonych w prawdziwym a nie wirtualnym sądzie. [6]



FUNDACJA bezpieczna cyberprzestrzeń

Tabletowe badziewie ze wschodu i zachodu

Specjaliści z NCC Group przebadali poziom bezpieczeństwa tabletów przeznaczonych dla dzieci, tabletów, które znajdują się na liście najbardziej popularnych zakupów gwiazdkowych. Jeden pochodził z Dalekiego Wschodu, drugi z Ameryki Północnej (zapewne należy czytać z Chin i USA). Wyniki są słabiutkie. Poziom bezpieczeństwa miejscami zerowy. Brak jakiegokolwiek szyfrowania przy przekazywaniu danych pomiędzy tabletem a producentem, co dotyczy danych osobowych rodziców i dzieci. Prawie to samo dotyczy haseł. Współdzielący sieć WiFi mają dostęp praktycznie do wszystkich informacji o komunikacji tabletu z Internetem - t.j. oglądanych stron a nawet możliwość aktualizowania stron, które dzieci mogą odwiedzać. No cóż producentom pozostaje chyba już tylko oświadczenie, że pełna otwartość wymienianych danych to nowatorski pomysł na kontrolę rodzicielską. [7]

[1] http://tinyurl.com/cybsecurity-zawor-2-1
[2] http://tinyurl.com/cybsecurity-zawor-2-2
[3] http://tinyurl.com/cybsecurity-zawor-2-3
[4] http://tinyurl.com/cybsecurity-zawor-2-4
[5] http://tinyurl.com/cybsecurity-zawor-2-5
[6] http://tinyurl.com/cybsecurity-zawor-2-6
[7] http://tinyurl.com/cybsecurity-zawor-2-7

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