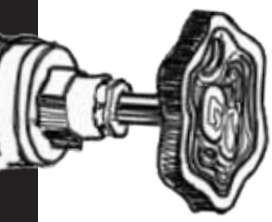
8/2014

FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 8/2014

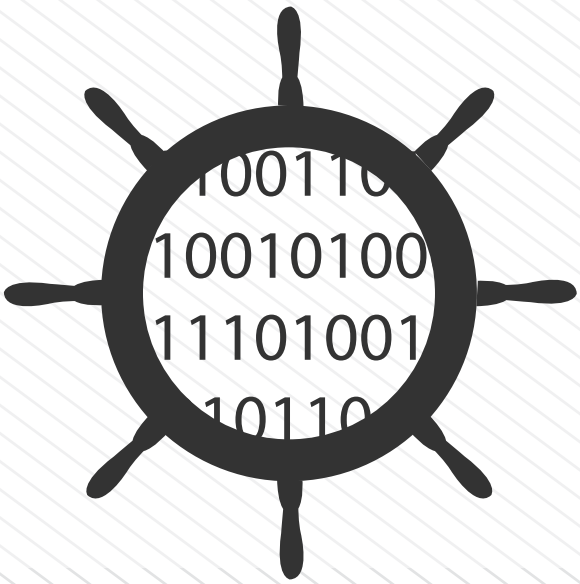
Telefon robi sweet-focię złodziejowi

Jeden ze studentów w Wielkiej Brytanii utracił telefon. Został mu skradziony z kieszeni płaszcza. Złodziej natknął się jednak na sprytne zabezpieczenie w telefonie. Wpisując kilkukrotnie błędny PIN spowodował, że telefon zrobił zdjęcie nowemu „właścicielowi" i wysłał je do starego właściciela. To nie oznacza, że telefon został już odzyskany, ale zawsze łatwiej szukać nowego właściciela, a gdyby się jeszcze okazało, że do zdjęcia dodawany jest geo-tag i możemy namierzyć obecne

miejsce właściciela na mapie to jesteśmy już znacznie bliżej. Jak zobaczysz kogoś wstukującego nerwowo PIN i ubranego w kominiarkę to znaczy, że natrafiłeś na złodzieja, który czytał „Zawór Bezpieczeństwa". [1]

Haker na okręcie atomowym

27 letni Mikołaj Paweł Rycerz (Nicholas Paul Knight) służący na USS Harry S. Truman - amerykańskim lotniskowcu atomowym, okazał się być cyberprzestępcą posługującym się wieloma nickami (Intertia, Logic, nickmc01, Solo, INTER7IA, |Logic|. Używał ich jako lider grupy hakerskiej „Digi7al" (wcześniej „Hav0k"). Grupa działała aktywnie od wielu lat - sam Knight działał w niej od 16-tego roku życia. Członkowie „Digi7al" mieli na koncie nie byle jakie



zdobycze: systemy amerykańskiej marynarki wojennej (tu Knight miał dość blisko), systemy Amerykańskiej Narodowej Agencji Wywiadu Kosmicznego, systemy Departamentu Bezpieczeństwa Narodowego, systemy

słynnego laboratorium w Los Alamos, policji kanadyjskiej, AT&T i ... muzyka Rashoda Holmes'a. Ostatecznie sami trafili na celownik wymiaru sprawiedliwości i zasiądą na ławie oskarżonych sądu w Tulsa (Oklahoma). Nagrania Rashoda mogą się przydać na długie spacery w słonecznym więziennym wybiegu. [2]

Cyber-pracownik miesiąca dostanie Ferarri. A co z lotem na marsa?

To, że cyberprzestępcy kopiują znane z rynku rozwiązania marketingowe i wdrażają je w świecie przestępczym wiadomo od dawna. Na przykład undergroundowe serwisy aukcyjne oferują exploity, usługi włamań itp. Kolejny pomysł wdrożył jeden z liderów świata cyberprzestępczego. Za najlepszy scam (*internetowe oszustwo przyp.red.*) oferuje on samochód marki Porsche albo Ferrari. Konkurs skierowany jest do grup cyberprzestępców, którzy chcieliby się pochwalić swoimi dokonaniami. Nagroda wydaje się niesamowita, ale zaraz, zaraz ... cyberprzestępca w wyniku sprawnego oszustwa potrafi pozyskać setki albo tysiące danych kart kredytowych, a każda z nich jest do sprzedania w podziemiu za kilkaset dolarów, to oferta dla „pracownika miesiąca" może okazać się nawet śmieszna. Stróże prawa powinni ogłosić szybko lepszą nagrodę - miejsce w zespole wybranym do lotu na Marsa. Bez prawa rezygnacji rzecz jasna. [3]

Pin-y w żyłach

Jak się dowiadujemy Polska staje się jednym z prekursorów powszechnego wykorzystania mało znanej metody biometrycznej. Do końca roku w dwustu bankomatach na terenie Polski możliwe będzie autoryzowanie swojej karty w bankomacie z wykorzystaniem czytnika biometrycznego, który sprawdza rozkład żył w naszym palcu. Jest to cecha biometryczna, która cechy unikalności nabywa już w okresie prenatalnym. Wcześniej na dużą skalę implementowano takie rozwiązanie w Turcji a w niektórych krajach takie rozwiązanie stosuje się nawet bezpośrednio przy zakupach, „płacąc" przyłożeniem palca do skanera. No cóż - pozostaje nadzieja, że cyber-złodzieje nie będą potrafili z bankomatu wyżyłować nie swoich pieniędzy. Wszystkich, którzy mają złe zamiary śpieszymy informować, że palce bez wykazującego pulsu i odnotowanym spadkiem hemoglobiny (tak dziej się po jego odcięciu) nie pozwoli na autoryzację. [4]

Agent FBI z trawką przy klawiaturze

Amerykański FBI ma poważny problem. Proces rekrutacji wskazuje na to, że wśród najlepszych kandydatów do walki z cyberprzestępcami jest wielu takich, którzy nie przechodzą pomyślnie testu,

w którym muszą zadeklarować, że w ostatnim okresie nie pobudzali się środkami odurzającymi. Problem wyszedł na jaw w sytuacji kiedy okazało się, że trzeba pilnie zatrudnić około 2 tysięcy specjalistów do ścigania cyberprzestępców. Ci dobrze rokujący również sobie popalają - głównie marihuanę. Cyberprzestępców przybywa, a „czystych" kandydatów na ichściganie jak na lekarstwo. Wychodzi na to, że nie będzie wyjścia i trzeba będzie zaakceptować specjalistów popalających trawkę. Ciekawe, czy wśród właściwości marihuany pojawią się opisy z kategorii „zastosowanie w cyberbezpieczeństwie"? [5]

Szyfrowanie, kodowanie i solenie ...buta

Wyjaśnienie znaczenia i konsekwencji niektórych z pojęć bezpieczeństwa nie jest zadaniem łatwym. Problem dodatkowy pojawia się przy tematach szczególnie trudnych - na przykład funkcji

związanych z szyfrowaniem. Powszechnie mówi się, że dane zostały zaszyfrowane i to ma wyjaśnić wszystko, tzn. przede wszystkim to, że jest bezpiecznie. A wcale nie zawsze bezpiecznie jest, np: jeśli chodzi o przechowywanie haseł. Zaszyfrowanie hasła to jak włożenie buta do pudełka. Pudełko można otworzyć i buta zobaczyć, czyli odczytać hasło. Dlatego hasła trzeba kodować (chodzi o funkcję skrótu, czyli o tzw. "hush") i solić. OK - kodować - tak.
Ale solić? To prawdziwa konfuzja. Posolenie hasła ma doprowadzić do jego najwyższego poziomu bezpieczeństwa. O co chodzi? Znaleźli się tacy, którzy w dość przejrzysty i interesujący sposób wyjaśnili - do nich odsyłamy - przedstawia ich Graham Cluley. [6]

[1] http://tinyurl.com/nhg8sbr
[2] http://tinyurl.com/kdzr5xf
[3] http://tinyurl.com/l5daslx

[4] http://tinyurl.com/l4yy9zc
[5] http://tinyurl.com/qjk6ysu
[6] http://tinyurl.com/lw9bsxt

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