White Hat – cyberdżentelmeni na tropie

Kategoria: Styl życia
Opublikowano: sobota, 23, maj 2020 07:46
Alicja Cisowska

Dżentelmeni jednak nie wyginęli. W dobie powszechnej cyfryzacji możemy liczyć na cyberdżentelmenów – czyli tzw. białe kapelusze (ang. White Hat).

Okazuje się, że zainteresowania informatyczne i instynkt detektywa można wykorzystać także w cyberprzestrzeni, np. przy tropieniu podatności oprogramowania na ataki i błędy w aplikacjach. Dlaczego to ważne? Nawet niewielka podatność lub niewidoczny na pierwszy rzut oka błąd systemu mogą umożliwić cyberprzestępcom uzyskanie nieuprawnionego dostępu do naszych danych. Nad tym, aby tak się nie stało czuwają między innymi tzw. hakerzy w białych kapeluszach.

White hat dzieli się swoją wiedzą. Wykorzystuje ją, by podnieść poziom cyberbezpieczeństwa danego systemu, a nie po to, by ten system zablokować, zniszczyć dane, czy uzyskać nieuprawniony dostęp do np. rachunków bankowych. To dlatego hakerzy w białych kapeluszach są nazywani etycznymi hakerami. Czerpią satysfakcję nie tylko z odkrywania błędów i „tylnych wejść" do systemów teleinformatycznych, ale również z uczestnictwa w procesie ich usuwania. W tym celu informacje o wykrytych problemach przekazują bezpośrednio do administratorów systemów, producentów oprogramowania, a także właściwych zespołów reagowania na incydenty bezpieczeństwa – CSIRT/CERT.

- *Wszystkie systemy informatyczne wymagają stałego monitorowania i testowania. Na każdym etapie – przed produkcją, podczas produkcji, jak i w fazie po oddaniu do użytku. Nie ma systemu idealnego. Regularnie słyszymy o tym, że różnego rodzaju podatności są wykrywane w nawet najbardziej zaawansowanych systemach* – mówi Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji. – *Dlatego nieocenioną rolę pełnią ci, którzy te podatności wychwytują i informacje na ich temat przekazują do zainteresowanych stron* – dodaje.

O tym, jak potrzebny jest tzw. etyczny haking przekonujemy się w praktyce. Ostatnio takim właśnie hakerem w białym kapeluszu okazał się inżynier i analityk rozwiązań chmurowych w firmie Intel Polska – Ciprian Alexandru Pitis. Wykrył dwie podatności w implementacji aplikacji webowej do podpisywania plików podpisem zaufanym w serwisie moj.gov.pl. Poinformował o tym nasz Departament Cyberbezpieczeństwa i zespół CSIRT NASK.

Przekazane przez niego (20 kwietnia) informacje zostały wykorzystane w dodatkowych analizach przeprowadzonych przez Centralny Ośrodek Informatyki (COI). Eksperci COI 29 kwietnia wprowadzili poprawki uniemożliwiające wykorzystanie wykrytych podatności.

- *Nikt nie jest doskonały. Dlatego cieszymy się, że są takie osoby i firmy, które kierując się profesjonalizmem i dobrem wspólnym analizują systemy, wychwytują podatności i reagują* – mówi dyrektor Robert Kośla. – *Tego typu działania, nakierowane na poprawę bezpieczeństwa oprogramowania i usług, z których korzysta na co dzień wiele przedsiębiorstw i użytkowników - są de facto najlepszą praktyką partnerstwa publiczno-prywatnego w cyberbezpieczeństwie* - dodaje.

Takie partnerstwo umożliwia budowę jeszcze efektywniejszego krajowego systemu cyberbezpieczeństwa, który ma wpływ na nas wszystkich, a nie tylko operatorów usług kluczowych czy dostawców usług cyfrowych.

Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty – to jeden z głównych celów Strategii Cyberbezpieczeństwa RP na lata 2019-2024.

Zaplanowane testy i audyty bezpieczeństwa to kluczowe elementy jego realizacji.

Co więcej, w ramach Strategii - „w celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa" - propagowane będzie testowanie zabezpieczeń w modelu tzw. „bug-bounty", czyli najprościej mówiąc – „polowanie" na błędy.

Źródło: MC