aut. Tomasz Fastyn 04.08.2016

US NAVY ZGŁĘBIA TECHNIKI HAKERÓW

W zeszłym miesiącu na terenie Panama City, gdzie mieści się siedziba jednego z centrów wojennych marynarki wojennej Naval Surface Warfare Center Panama City Division (NSWC PCD) odbyły się zawody Capture The Flag. Powodem organizacji zawodów miało być według organizatorów pokazanie w jak łatwy i prost sposób hakerzy mogą łamać zabezpieczenia oraz hasła użytkowników.

Organizatorzy całego przedsięwzięcia Daniel Jermyn oraz Trevor Phillips twierdzą, że takie zawody w których biorą osoby, które w przyszłości będą odpowiadać za bezpieczeństwo marynarki wojennej, powinny znać schematy działania hakerów. Jednocześnie CTF ma pokazać, jak łatwo przy pomocy prostych i dostępnych na rynku narzędzi można wykorzystać wszelkie luki w systemach informatycznych. Pokazanie uczestnikom jak działają hakerzy i jakich narzędzi używają oni do łamania tzw. bezpiecznych haseł. Takie mechanizmy i działania według organizatorów mają uświadomić pracowników odpowiadających za cyberbezpieczeństwo, że powinni oni świadomiej dbać o poziom zabezpieczeń.

– Zawody CTF pokazuję jak ważne jest zabezpieczenie własnego systemu. Hakerzy zawsze próbują włamać się do infrastruktury informatycznej, wyszukują luki czy wady, które pozwolą im na wykonanie ataku – powiedział Matthew Chastain z NSWC PCD.

Jak czytamy na portalu dvidshub.com same zawody skupiły się na pokazaniu jak wyglądałby scenariusz ataku na jeden z bezzałogowych pojazdów. Podczas takiego scenariusza zostały użyte prawdziwe narzędzia oraz mechanizmy wykorzystywane przez hakerów podczas codziennych włamań na serwery i urządzenia podłączone do sieci.

Powód dla którego organizatorzy zdecydowali się na przeprowadzenia takich zawodów wśród programistów oraz osób odpowiedzialnych za działanie sieci jest według nich dosyć prozaiczny. Ponieważ obecnie podczas szkoleń a nawet nauki na uczelniach, są oddzielani od specjalistów cyberbezpieczeństwa. Powoduje to sytuacje w których tworząc infrastrukturę oraz sieci internetowe mają niewielkie pojęcie o mechanizmach bezpieczeństwa, które powinny mieć miejsce.

– Obecnie, programiści oraz developerzy tworzą rozwiązania bez udziału osób odpowiedzialnych za bezpieczeństwo informatyczne. Mechanizmy cyberbezpieczeństwa mogą zostać zaimplementowane podczas procesów pisania i tworzenia. Staramy się zwracać uwagę programistów na problemy związane z tworzeniem infrastruktury, tak aby mogli współpracować z innymi ekspertami w celu zapewnienia odpowiednich mechanizmów bezpieczeństwa – powiedziała Kate Magilo z NSWC PCD.

Czytaj też: Już w listopadzie największe zawody cybernetyczne na terenie Europy