https://wyborcza.pl/magazyn/7,124059,27500454,do-skutecznego-i-dotkliwego-cyberataku-wystarczy-tani-laptop.html

Wojciech Cellary 2021-08-28

Atak i obrona

Dawno temu za studenckich czasów uczęszczałem na obowiązkowe zajęcia ze studium wojskowego. Pamiętam jak dzielny major H., który miał wykłady ze sztuki wojskowej, mówił, że łatwiej jest się bronić niż atakować i że sił atakujących powinno być pięć razy więcej niż obronnych dla zapewnienia zwycięstwa.

To właśnie diametralnie się zmieniło w czasach internetu – to sił obronnych musi być o wiele więcej. Do skutecznego i bardzo dotkliwego cyberataku wystarczy tani laptop w rękach hakera, którym może być nawet student, byleby tylko miał odpowiednie umiejętności i trochę szczęścia. Za to obrona przed cyberatakiem wymaga wielkich nakładów, dużego zespołu ludzi i stałej pracy nad wykrywaniem i usuwaniem podatności współczesnych systemów cyfrowych na ataki. Systemy stają się coraz bardziej złożone – ludzkość nie wymyśliła niczego bardziej skomplikowanego niż połączone ze sobą systemy informatyczne. Te systemy muszą ze sobą współpracować, bo dzisiaj wszystko co może być połączone, jest dla naszej wygody połączone, ale były projektowane niezależnie od siebie, przy różnych założeniach, z przeznaczeniem dla różnych celów, w dodatku w różnym czasie, gdy różne były znane zagrożenia dla bezpieczeństwa. Dlatego są one łatane, rozbudowywane, dostosowywane i zabezpieczane, ale to zwiększa ich złożoność, a większa złożoność to więcej potencjalnych podatności na ataki. Wyjściem z tego błędnego koła jest w pewnym momencie tylko napisanie pewnych systemów od nowa przy nowych, współczesnych założeniach, nawet kosztem ich zgodności ze starym oprogramowaniem.

Niektóre podatności na ataki są poza zasięgiem informatyków. Techniczne zabezpieczenie systemów przed naiwnością i brakiem wiedzy użytkowników komputerów graniczy z niemożliwością. Atak na użytkownika jest o wiele prostszy niż atak na serwer. Wystarczy na przykład zagrać na jego chciwości, informując go o wielkim spadku od nieznanego wujka z Ameryki lub możliwości odebrania niezamówionej paczki dużej wartości. Albo próżności, mówiąc o wygranej wielkiej nagrodzie, albo strachu, że zostanie pozbawiony jakichś usług informatycznych – zawsze pod jakimś warunkiem, na przykład wejścia na podany link, rzekomo prowadzący do jego konta w banku, a tak naprawdę do udającej stronę banku szalbierczej strony, służącej tylko do uzyskania jego danych, a później do podszycia się pod niego i okradzenia go. Atakujące mejle można wysłać do setek tysięcy potencjalnych ofiar, bo to

niewiele kosztuje. Za to każdy, kto da się nabrać, może być okradziony przez złodzieja zwanego hakerem.

Jeśli według takiego schematu przeprowadzi się skuteczny atak na osobę z rozszerzonymi uprawnieniami w systemie informatycznym, to można potem na przykład zaszyfrować serwer i żądać okupu. Takie rozszerzone uprawienia mają informatycy administrujący systemami, ale oni wiedzą na czym polegają takie ataki. Często mają je jednak również kierownicy, dyrektorzy i prezesi z racji pełnionych funkcji. Jeśli nie mają odpowiedniej wiedzy informatycznej, to są największym zagrożeniem dla swoich systemów.

Wrócę jeszcze do majora H. Jako studenci politechniki byliśmy bardzo zainteresowani sztuką i techniką wojskową, więc zadawaliśmy majorowi pytania. Na przykład – czy z dwóch półautomatów można zrobić jeden automat?