Heartbleed zagrożeniem dla internetowego e-handlu

17 kwietnia 2014

Złowrogie ostrzeżenia o Heartbleed, który jest poważnym zagrożeniem dla bezpieczeństwa internetu, dotykającym miliony stron internetowych, odbija się echem w całym internecie. Mówi się, że Heartbleed opisany jako błąd w OpenSSL, technologii szyfrowania open source, stosowanej przez większość serwerów internetowych, jest zagrożeniem dla internetowego e-handlu przez HTTPS.

Błąd „może dać hakerom dostęp do danych osobowych, takich jak numery kart kredytowych, nazw użytkownika, hasła, i co może najważniejsze, klucze kryptograficzne, które pozwalają hakerom podszywać się lub monitorować serwery „, pisze Lily Hay Newman.

Błąd został odkryty przez naukowca Google w Codenomicon, fińskiej firmy specjalizującej się w rozwoju „narzędzi typu Fuzz", zapewniających bezpieczeństwo sieci komputerowych. Baza klientów Codenomicon obejmuje rządy i przemysł obronny i jak piszemy poniżej firma ma podejrzane koneksje z administracją Obamy, Departamentem Bezpieczeństwa Wewnętrznego DHS oraz FBI.

Obecny szum medialny nt Heartbleed wpisuje się w trwającą kampanię propagandową rządu dążącą do stworzenia publiczno-prywatnej infrastruktury cyberbezpieczeństwa.

Ostatnie ostrzeżenie pochodzi z seminarium dyrektora ds. Komunikacji Globalnej Praktyki Energetycznej Willisa, które odbyło się w Londynie. Powiedział, że „energetyka siedzi na niezabezpieczonym niewypale ze strony niepewnych ataków cybernetycznych", w dużej mierze z powodu internetowych systemów kontroli, które są rutynowo niepewnie.

W 2010 r., działania mające na celu przedstawienie Internetu

jako podatnego na ataki i potrzebującego rządowej ochrony przyjęły kształt symulowanego cyberataku. Gra wojenna została zorganizowana przez Bipartisan Policy Center będącego think tankiem sponsorowanym przez „spółki które są zainteresowane finansowo przyszłością cyberbezpieczeństwa- General Dynamics jest jedną z firm- ale także inne firmy, których transakcje są siłą napędową amerykańskiej gospodarki, a którym zależy na budowaniu poczucia pilności działań wśród społeczeństwa i polityków," według Marca Ambindera z gazety The Atlantic.

Cyberataki często zbiegają się w czasie by podkreślić rządowe rozmowy i przepisy dotyczące cyberbezpieczeństwa. Na przykład, w lutym, bezprecedensowy atak typu Denial of Service został przeprowadzony kilka dni po tym jak ustawa dotycząca narodowego cyberbezpieczeństwa i ochronie infrastruktury krytycznej trafiła do parlamentu. Legislacje, wspierane przez Republikanów i Demokratów, kodyfikują „partnerstwo między prywatnym sektorem i DHS."

[…] Wcześniej w tym miesiącu, były senator Evan Bayh, demokrata ze stanu Indiana, powiedział American Bar Association sekcji prawa międzynarodowego, podczas wiosennego spotkania 2014 w Nowym Jorku, że jest mało prawdopodobne by w tej sesji Kongres przepchnął ustawodawstwo cyberbezpieczeństwa.

„Myślę, że jest mało prawdopodobne by nastąpiły działania legislacyjne" powiedział Bayh. „To niedobrze. Prawdopodobnie musi dojść do cyberataku, który w jakiś sposób z sukcesem wyrządzi znaczną szkodę dla kraju, zanim byłbym w stanie pogodzić debatę w Waszyngtonie na temat legislacji."

Bayh powiedział, że duży cyberatak spowoduje prawdopodobnie wprowadzenie „niektórych obowiązkowych norm, które będą niczym w porównaniu z tym, co zaproponowano do tej pory. Ponieważ my zawsze reagujemy z przesadą po tym jak zostaliśmy zaatakowani, i obie strony muszą to zrozumieć, że to jest to, co nadchodzi," powiedział.

Bayh, który siedział na senackiej komisji ds. wywiadu, zasiada obecnie w radzie doradczej CIA. W związku z tym jego ostrzeżenia i przewidywania, wyrażone jako pewnik, niosą w sobie niezwykłą wagę.

Wreszcie, należy zauważyć, że Howard Schmidt ,były koordynator ds. cyberbezpieczeństwa i specjalny asystent Obamy, zasiada w zarządzie firmy Codenomicon.

Schmidt, który również pracował dla FBI i Departamentu Bezpieczeństwa Wewnętrznego, „był odpowiedzialny za międzyagencyjną koordynację oraz rozwój i skoordynowane wdrażanie polityki cyberbezpieczeństwa z federalnymi, stanowymi, lokalnymi, międzynarodowymi i prywatnymi partnerami sektora cyberbezpieczeństwa," podaje strona firmy Codenomicon Defensics.

To wiele nam mówi o firmie powiązanej z Google, z jej znanymi, wywiadowczymi koneksjami, mającej za członka zarządu człowieka związanego bezpośrednio z inicjatywami cyberbezpieczeństwa i powiązaniami z DHS, FBI i administracją Obamy, która odkryła błąd prosząc o rządową interwencję.

Autor: Kurt Nimmo
Źródło oryginalne: Infowars.com
Źródło polskie: PrisonPlanet.pl