aut. Tomasz Fastyn 27.02.2017

NSA NADAL Z DOSTĘPEM DO INFORMACJI O BŁĘDACH ZERO-DAY

Proces zbierania i przechowywania luk w oprogramowaniu typu zero-day przez NSA nie zmieni się w najbliższym czasie. Eksperci krytykują zachowanie procedury *vulnerabilities equities process* (VEP), która pozwala agencjom na zachowywanie informacji dotyczących krytycznych luk do dalszych działań operacyjnych.

Po zmianie administracji Białego Domu wielu ekspertów sądziło, że prawo pozwalające w nieograniczony sposób przechowywać informacje o krytycznych lukach przez NSA ulegnie modyfikacji. Podczas ostatniej konferencji RSA, przedstawiciele rządu przekazali, że nie zostaną wprowadzone żadne zmiany w VEP.

Podobne procedury posiada także brytyjskie GCHQ. W obu agencjach takie działania są częścią rutynowych zadań, które pozwalają na przygotowanie odpowiedniej bazy informacyjnej, wykorzystywanej podczas operacji defensywnych i ofensywnych w cyberprzestrzeni.

Czytaj też: NSA wykorzystywała cyberataki do obrony własnej

Procedura VEP wywołuje wiele emocji zarówno po stronie administracji, która podkreśla, że działania są niezbędne, jak i po stronie sektora prywatnego, który zaznacza, że takie metody nikomu nie służą. Problemem w całej sprawie jest także wymiar bazy informacji o lukach, jaką przechowuje NSA.

Według ekspertów baza informacji jest znacznie mniejsza, niż wyobrażają ją sobie korporacje, zaś część rekordów jest wręcz niezbędna na wypadek działań obcych służb. Sprawie nie pomaga także zeszłoroczna działalność grupy Shadow Brokers, która próbowała sprzedać narzędzia wykradzione z urządzeń należących do Equation Group pracującej dla NSA. Część z nich zawierała podatności (luki w oprogramowaniu), o których producenci nie mieli żadnych danych. Miały klasę zero-day.