WYTYCZNE

w zakresie ochrony portali informacyjnych administracji publicznej

Jednym z wniosków wyciągniętych z ataków przeciwko systemom leżącym w domenie *gov.pl* jest brak możliwości zapewnienia monitorowania w czasie rzeczywistym obciążenia witryn, a co za tym idzie – szybkiego reagowania na incydent.

Niezbędne jest ustanowienie stałych kontaktów z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz obowiązek wdrażania zaleceń CERT.GOV.PL.

Doraźnie należy obligatoryjnie zastosować, w zakresie zawieranych umów na prowadzenie portali, zapisy umożliwiające:

- wdrożenie systemów eliminacji ruchu anonimizowanego (tj. TOR, znane Anon–oraz Open – Proxy, znane Anon – VPN, itp.) oraz wymuszenie ciągłej aktualizacji tych mechanizmów;

- możliwość całkowitego filtrowania ruchu dotyczącego określonych typów pakietów lub całych protokołów (np. UDP lub ICMP);

- wprowadzenie odpowiedzialności firmy hostującej za zapewnienie ciągłości działania powierzonego serwisu (w przypadku operatora zapewniającego jedynie połączenie – minimalną, gwarantowaną przepustowość łącza);

- użycie mechanizmów automatycznego (oraz na żądanie) przełączania wersji witryn (strona dynamiczna – strona statyczna – informacja o przerwie techniczne) w zależności od poziomu wysycenia łącza oraz obciążenia serwera świadczącego usługi publiczne;

- dla serwisów o wskazanej wyżej dostępności usług wprowadzenie mechanizmów rozkładających ruch w przypadku dużego natężenia pomiędzy grupę serwerów;

- wdrożenie rozwiązań kontrolujących zawartość strony (od strony serwera) i raportujących o możliwości nieuprawnionej modyfikacji treści serwisu wraz z możliwością automatycznego zablokowania wyświetlania zmienionej strony.

Mając na względzie konieczność utrzymania kontaktów urzędników administracji rządowej z podmiotami zewnętrznymi za pomocą internetowej poczty elektronicznej należy wdrożyć niezbędne procedury bezpieczeństwa nie tylko po stronie systemowej ale także użytkownika, W tym celu należy:

- w związku z powtarzającymi się atakami słownikowymi na konta pocztowe jednostek administracji państwowej, zaleca się zablokowanie dostępu do tych kont z sieci Internet a pozostawianie jedynie możliwości logowań sieci wewnętrznej;

- w przypadku, gdy dostęp do poczty elektronicznej jest niezbędny z sieci Internet, należy go zrealizować poprzez szyfrowane tunele VPN;

- niezbędna jest zmiana haseł użytkowników na mało podatne na tego typu ataki zawierające duże, małe litery, znaki specjalne oraz cyfry;

- z uwagi na próby ataku na systemy i użytkowników po stronie administracji rządowej poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych załączników. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony WWW, zaleca się aby nie otwierać załącznika ani korzystać bezpośrednio z przesłanych odnośników;

- w okresie średnioterminowym administratorzy systemów pocztowych powinni wdrożyć rozwiązania zabezpieczające oparte o kaskady oprogramowania antywirusowego, silne mechanizmy antyspamowe, filtrowanie i blokowanie wysyłanej i odbieranej poczty wg zdefiniowanych warunków (ochrona przed wysyłką dokumentów, informacji wewnętrznych);

- wszelkie podejrzane wiadomości w całości (wraz z nagłówkami i załącznikiem)należy przesłać do weryfikacji do zespołu CERT.GOV.PL na adres incydent@cert.gov.pl;

Dodatkowo należy bezwzględnie wdrażać w życie zalecenia i wytyczne publikowane okresowo przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, a także przesyłane bezpośrednio do administratorów systemów. W przypadku jakichkolwiek podejrzeń wystąpienia incydentu użytkownik powinien niezwłocznie skontaktować się z lokalnym administratorem, natomiast administratorzy z zespołem CERT.GOV.PL.