Serwisy publiczne w niebezpieczeństwie

Kategoria: Aktualności
Opublikowano: niedziela, 11, wrzesień 2011 00:00
Tadeusz Narkun

Serwis Samorządowy PAP wystąpił z listem do MSWiA, pytając o bezpieczeństwo samorządowych stron internetowych w kontekście ostatnich ataków, o których również pisaliśmy w naszym serwisie. W odpowiedzi resort stwierdził, że większość jednostek umieszcza swoje strony podmiotowe na serwerach świadczących usługi hostingu, a więc obowiązek zapewnienia odpowiedniego bezpieczeństwa musi być uzgodniony pomiędzy daną jednostką a podmiotem świadczącym daną usługę.

Zagrożenie dla samorządowych stron BIP jest wciąż realne - wynika z informacji Rządowego Zespołu Reagowania na Incydenty Komputerowe, cert.gov.pl. Firma hostingowa nie wdrożyła zaleceń bezpieczeństwa - czytamy na stronie cert.gov.pl

W myśl rozporządzenia MSWiA, strony BIP powinny być chronione przez moduł bezpieczeństwa - rozwiązanie techniczne uniemożliwiające zniszczenie lub modyfikację informacji publicznych przez osoby nieuprawnione.

Jednostki zobowiązane do udostępniania informacji publicznych powinny respektować przepisy bezpieczeństwa. Nakładają one obowiązek stosowania rozwiązań chroniących przed celowym spowolnieniem lub uniemożliwieniem dostępu do zasobów tych stron.

Zapobiec włamaniom w przyszłości mają „standardy bezpieczeństwa dotyczące funkcjonowania systemów w cyberprzestrzeni", wprowadzana w obszarze administracji publicznej. Pierwszym dokumentem poruszającym tę problematykę jest Polityka Bezpieczeństwa Cyberprzestrzeni RP. Celem zapewnienia administracji publicznej ochrony przed cyberzagrożeniami, w Agencji Bezpieczeństwa Wewnętrznego funkcjonuje Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL, za pośrednictwem którego można zgłaszać m.in. włamania lub próby włamań oraz inne przypadki naruszenia bezpieczeństwa teleinformatycznego. To właśnie ten zespół przeprowadził analizę i zidentyfikował przyczyny ostatnich włamań oraz przekazał zalecenia firmie hostingowej, m.in. zmiany konfiguracyjne oraz wprowadzenie filtrowania danych przekazywanych w parametrach do skryptów php.

Firma hostingowa podjęła próbę ponownego uruchomienia serwisów internetowych, ale nadal występowały błędy pozwalające na przełamanie zabezpieczeń. Jak wynika z informacji na stronie cert.gov.pl, zalecenia nie zostały wdrożone.

Według MSWiA problem powinna rozwiązać budowa Scentralizowanego Systemu Dostępu do Informacji Publicznej (SSDIP) i wprowadzenie jednolitego standardu informacji na stronach podmiotowych Biuletynu Informacji Publicznej.

Zdaniem resortu, poprzez wprowadzenie jednolitego szablonu stron BIP usprawni się mechanizm gromadzenia, udostępniania i prezentacji informacji publicznych oraz wprowadzony zostanie jednolity system identyfikacji wizualnej. Dodatkowo poprzez wprowadzenie nowego systemu zwiększy się bezpieczeństwo danych umieszczanych w BIP.

Zastosowane mechanizmy bezpieczeństwa stron podmiotowych BIP w ramach SSDIP gwarantowane są dzięki użyciu sprzętu najwyższej jakości. Dodatkowo w SSDIP zostało zastosowane zabezpieczenie programowe o wysokim standardzie. Dla wzmocnienia bezpieczeństwa SSDIP korzysta z systemu uprawnień ePUAP. Skorzystanie z SSDIP pozwoli urzędom oraz innym instytucjom na wywiązywanie się z ustawowego obowiązku bez konieczności ponoszenia kosztów outsourcingu, czy budowy i utrzymania aplikacji.

Kategoria: Aktualności
Opublikowano: niedziela, 11, wrzesień 2011 00:00
Tadeusz Narkun
Odsłony: 1661

Informacje publiczne na stronach podmiotowych BIP w ramach Scentralizowanego Systemu Dostępu do Informacji Publicznej może zamieszczać wyłącznie administrator strony podmiotowej BIP lub redaktor tej strony. Zadanie to wykonywać mogą jedynie pracownicy podmiotów publicznych posiadających konto na platformie ePUAP.

Kilka słów komentarza: Następuje atak na strony samorządowe, a więc publiczne. Po zbadaniu charakteru ataku przez Rządowy Zespół Reagowania na Incydenty Komputerowe firma hostingowa próbuje ponownie uruchomić komputery. Próba jest nieudana, bo nadal występowały błędy zabezpieczeń. Okazuje się, że firma nie wdrożyła zaleceń (sic!). Czego to dowodzi? Trzeba budować systemy bezpieczne, szczelne i pewne, aby nie wyciekały dane. Można to robić różnymi sposobami. Najważniejszy okazuje się jednak człowiek i jego odpowiedzialność. To trochę tak jak z najnowszym samochodem, wyposażonym w najnowocześniejsze środki bezpieczeństwa, a i tak ulega on wypadkowi. Dlaczego? Ponieważ w mózgu kierowcy tego samochodu nie było klapki bezpieczeństwa, a bez niej najbardziej wymyślne mechanizmy są na nic.