REKOMENDACJA MAC/SEC/1/15

ŚRODKI IDENTYFIKACJI W ADMINISTRACJI PUBLICZNEJ

KWIECIEŃ 2015

Spis treści

Podmiot realizujący zadania publiczne jest zobowiązany do zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji

Wstęp

Zgodnie z §20 pkt. 1 ***Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*** (Dz.U.2012.526 tj.) podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zgodnie z §20 pkt. 2 Rozporządzenia zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

W związku z koniecznością niezwłocznego spełnienia przez podmioty realizujące zadania publiczne wymagań związanych z zapewnieniem odpowiedniego poziomu bezpieczeństwa przy dostępie do systemów i aplikacji zachodzi potrzeba wskazania najlepszych praktyk w zakresie środków identyfikacji, które należy zastosować przy dostępie pracowników do systemów back office, jak również podniesienia bezpieczeństwa przy wymianie korespondencji elektronicznej pomiędzy podmiotami publicznymi.

Głównymi adresatami zaleceń są Dyrektorzy Generalni i Kierownicy Jednostek Organizacyjnych.

Podmiot realizujący zadania publiczne jest zobowiązany do zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie

ZALECENIE 1

Środki identyfikacji, które należy zastosować przy dostępie pracowników do systemów back office

***Zaleca się* wdrożenie w podmiotach publicznych mechanizmów uwierzytelniania zbudowanych w oparciu o architekturę PKI *(public key infrastructure)*, wykorzystującą certyfikaty X.509 wraz z zastosowaniem kart inteligentnych „*Smart Card*" do ochrony kluczy prywatnych powiązanych z certyfikatami. Ponadto zaleca się zintegrowanie zastosowanych kart inteligentnych z elektronicznym systemem kontroli dostępu stosowanym w budynkach w celu zapewnienia zabezpieczenia fizycznego dostępu do konsoli zalogowanego użytkownika.**

Termin na wdrożenie zalecenia: IV kw. 2016 r.

Korzyści zalecanego rozwiązania

Wprowadzenie ustandaryzowanych środków identyfikacji stosowanych przy dostępie pracowników do systemów back office umożliwi podniesienie wspólnego poziomu bezpieczeństwa w systemach teleinformatycznych podmiotów publicznych.

Zastosowanie architektury PKI jest powszechnie stosowanym mechanizmem uwierzytelniania a odpowiednio zaprojektowana i wdrożona architektura umożliwia budowanie nowych bezpiecznych usług przez podmioty realizujące zadania publiczne.

Umieszczenie kluczy prywatnych certyfikatów wykorzystywanych do uwierzytelniania na kartach inteligentnych (Smart Card) nie tylko zabezpiecza je przed skopiowaniem ale również wprowadza dodatkową warstwę zabezpieczeń w postaci ochrony kluczy np.: za pomocą kodu PIN. Ponadto wykorzystanie tak chronionego mechanizmu uwierzytelniania rozszerza mechanizm standardowego logowania za pomocą mechanizmu login – hasło wprowadzając drugi składnik w postaci fizycznego nośnika jakim jest karta. W tym przypadku mamy do czynienia z modelem w którym rolę fizycznie posiadanego składnika „*something you have*" pełni karta inteligentna, natomiast rolę drugiego składnika „*something you know*", który jest znany tylko użytkownikowi pełni sekret wykorzystywany przez mechanizm ochrony kluczy na karcie np.: kod PIN.

Jednocześnie zalecane jest zintegrowanie wykorzystywanych kart inteligentnych z elektronicznym systemem kontroli dostępu, który powinien wymagać użycia karty w celu opuszczenia chronionej strefy przez pracownika, aby tego dokonać użytkownik musi zabrać kartę ze sobą co automatycznie wymusza zabezpieczenie stacji końcowej (np.: zablokowanie sesji użytkownika)

Podsumowanie

Zalecane jest wzmocnienie mechanizmów uwierzytelniania stosowanych w systemach back office podmiotów realizujących zadania publiczne.

ZALECENIE 2

Podniesienie bezpieczeństwa poczty elektronicznej pomiędzy podmiotami publicznymi

Zaleca się powszechne wprowadzenie mechanizmu zapewnienia integralności i autentyczności korespondencji elektronicznej e-mail, wysyłanej z podmiotów publicznych za pomocą podpisywania jej przy użyciu nie kwalifikowanych certyfikatów elektronicznych w standardzie X.509, wydawanych z wewnętrznego centrum CA (*Certification Authority*) wchodzącego w skład struktury drzewa PKI (*Public Key Infrastructure*) podmiotu publicznego. Zaleca się integrację polityk certyfikacyjnych służących do wydawania certyfikatów z państwowym drzewem zaufania.

Termin na wdrożenie zalecenia: IV kw. 2016 r.

Podmiot realizujący zadania publiczne jest zobowiązany do zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na ochronie przed nieuprawnioną modyfikacją

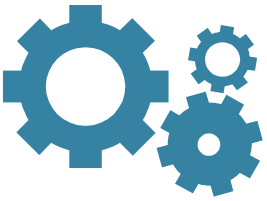
Korzyści zalecanego rozwiązania

W związku z powszechnością stosowania korespondencji elektronicznej wymienianej pomiędzy podmiotami publicznymi jak również kierowanej do podmiotów zewnętrznych i obywateli, zachodzi potrzeba zapewnienia odpowiedniego poziomu integralności i autentyczności korespondencji. W obecnych czasach korespondencja elektroniczna nadal pełni znacząca rolę przy przesyłaniu informacji drogą elektroniczną, jednak protokoły wykorzystywane do przesyłania wiadomości e-mail przez szereg lat nie uległy znaczącym zmianom uwzgledniającym postęp technologii i wzrost zagrożeń z nimi związanych. W związku z tym niezbędne jest wprowadzenie dodatkowej warstwy zapewniającej dostosowanie korespondencji elektronicznej za pomocą e-mail do aktualnie występujących wyzwań i zagrożeń. W szczególności należy mieć na uwadze, że często wiadomość elektroniczna jest traktowana jako źródło informacji a co za tym idzie naruszenie jej integralności i poufności może nieść za sobą szereg zagrożeń, oraz mieć negatywny wpływ na wizerunek podmiotu publicznego.

Podsumowanie

Celem zalecenia jest zapewnienie integralności i autentyczności korespondencji elektronicznej przesyłanej pomiędzy podmiotami publicznym jak również zbudowanie wspólnej architektury PKI umożliwiającej nawiązanie relacji zaufania pomiędzy poszczególnymi drzewami PKI podmiotów publicznych

Uwagi końcowe



W związku z rozwojem technologii cyfrowych oraz wyzwań i zagrożeń z nimi związanych niezbędne jest spójne wdrażanie mechanizmów w zakresie bezpieczeństwa cyfrowego w podmiotach publicznych zawartych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2012.526 tj.).

Przedstawione zalecenia zostały opracowane zgodnie z rekomendacją Nr 7, Zespołu do spraw metod uwierzytelniania: „*Zgodnie z treścią rozporządzenia eIDAS, które wejdzie w życie pierwszego lipca 2016 r., podpis elektroniczny służący do składania oświadczenia woli ma być wykorzystywany tylko do podpisywania dokumentów, natomiast do uwierzytelniania należy wykorzystywać odrębny certyfikat przypisany do innej pary kluczy*. ***W związku z tym powyższy Zespół rekomenduje, aby urzędy odeszły od praktyki wykorzystywania przy uwierzytelnianiu kluczy i certyfikatów przeznaczonych do podpisu elektronicznego***."