Ministerstwo Cyfryzacji
00-060 Warszawa
Królewska 27

Warszawa, 2019-01-24

DSP-VIII.5140.326.2018

Kierownicy Podmiotów Publicznych

INFORMACJA

Pismo

Szanowni Państwo,
w załączeniu przekazuję pismo Pana Karola Okońskiego Pełnomocnika Rządu do spraw Cyberbezpieczeństwa informujące o przesunięciu terminu wycofania algorytmu SHA-1 ze środowiska ePUAP i sytemu Profilu Zaufanego na dzień 31 marca 2019 r.
W przypadku, gdyby ten termin był za krótki, proszę o niezwłoczne przesłanie takiej informacji na adres e-mail: epuap_pz_sha2@mc.gov.pl, na który należy przesyłać również potwierdzenie gotowości do przejścia na funkcję skrótu SHA-256.
Przypominam, że brak wdrożenia algorytmu SHA-256 jest niezgodny z prawem, dlatego też w przypadku wdrożenia po stronie Państwa systemów tej funkcji skrótu proszę o niezwłoczne zaprzestanie korzystania z algorytmu SHA-1.

Z poważaniem,
Paweł Głośniewski
Zastępca

Dyrektora

Departamentu

Systemów Państwowych

Załączniki:

1. wdrożenie SHA-256 w ePUAP PZ.(2988322_3084656).pdf

Dokument został podpisany, aby go zweryfikować należy użyć oprogramowania do weryfikacji podpisu
Data złożenia podpisu: 2019-01-24T08:47:56.684Z
Podpis elektroniczny

Warszawa, dnia 23 stycznia 2019 r.

RZECZPOSPOLITA POLSKA
PEŁNOMOCNIK RZĄDU DO SPRAW CYBERBEZPIECZEŃSTWA

SEKRETARZ STANU
w MINISTERSTWIE CYFRYZACJI
Karol Okoński

DSP-VIII.5140.326.2018

Kierownicy Podmiotów Publicznych

Szanowni Państwo,

w związku z ustawową koniecznością, dostosowania wymagają wszystkie systemy teleinformatyczne wykorzystujące algorytm SHA-1, a jednocześnie współpracujące z profilem zaufanym oraz platformą ePUAP. Ministerstwo Cyfryzacji (MC) dokonało po swojej stronie niezbędnych modyfikacji i jest gotowe do wyłączenia rozwiązań stosujących algorytmu, który został rekomendowany do wycofania przez międzynarodowe instytucje badające bezpieczeństwo teleinformatyczne.

Rozumiejąc wagę i złożoność przedsięwzięcia Ministerstwo Cyfryzacji prowadziło w ubiegłym roku konferencje edukacyjno-informacyjne, dotyczące zaprzestania stosowania algorytmu SHA-1 w systemach ePUAP i profil zaufany. Informacje w tej sprawie były także sukcesywnie przekazywane do wszystkich zainteresowanych w tym również na Elektroniczne Skrzynki Podawcze podmiotów publicznych oraz za pośrednictwem poczty elektronicznej. Jednocześnie zostały udostępnione materiały z przeprowadzonych konferencji edukacyjno-informacyjnych w zakładce aktualności na stronach https://epuap.gov.pl oraz https://pz.gov.pl.

Pomimo tego, że MC dołożyło wszelkich starań, aby proces implementacji funkcji skrótu SHA-256 w zastosowaniach wymagających integracji z systemem profilu zaufanego lub ePUAP przebiegł szybko i skutecznie, w dalszym ciągu stwierdza się brak gotowości znacznej części instytucji publicznych do wyżej wymienionych zmian. Pragnę zaznaczyć, że brak wdrożenia algorytmu SHA-256 jest niezgodny z prawem (art. 137 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej zakazuje od 2 lipca 2018 r. stosowanie algorytmu SHA-1 przy składaniu zaawansowanych pieczęci elektronicznych) i niesie za sobą również niebezpieczeństwo kompromitacji wykorzystywanych przez Państwa systemów teleinformatycznych a w konsekwencji nawet może doprowadzić do „wycieku danych". Dlatego też podmioty gotowe na przystosowanie tej funkcji skrótu zobowiązuję do bezzwłocznego przejścia do jej wykorzystywania w swoim oprogramowaniu oraz systemach teleinformatycznych.

Mając na uwadze powagę przedsięwzięcia oraz w celu podjęcia wszystkich dostępnych przez MC środków niezbędnych do zachowania bezpieczeństwa systemów po raz kolejny zwracam się z prośbą do Państwa o przeprowadzenie w swoim urzędzie oraz jednostkach nadzorowanych i podległych czynności sprawdzających pod kątem tego, czy oprogramowanie i systemy dostarczone przez integratorów zostały dostosowane do wymienionego przepisu prawa tak, aby sygnowane

Pismo jest zgodne z wymaganiami WCAG 2.0 dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych, określonymi w załączniku nr 4 do 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. z 2017 poz. 2247)

przez Państwa dokumenty były podpisami elektronicznymi spełniającymi wymóg prawa oraz systemu standaryzacyjnego (ETSI TS 119 312).

Ostateczne wycofanie algorytmu SHA-1 ze środowiska ePUAP i sytemu profilu zaufanego zostaje przesunięte na dzień 31 marca 2019 r., brak dostosowania w tym terminie uniemożliwi komunikację z tymi systemami. W przypadku, gdyby ten termin był za krótki, proszę o niezwłoczne przesłanie takiej informacji na adres e-mail: epuap_pz_sha2@mc.gov.pl , na który należy przesyłać również potwierdzenie gotowości do przejścia na funkcję skrótu SHA-256. Ponadto w przypadku wdrożenia już po stronie Państwa systemów funkcji skrótu SHA-256 proszę o rozpoczęcie korzystania z nowego rozwiązania.

Zachęcam także do nawiązania współpracy z Service Desk Centralnego Ośrodka Informatyki. Formy kontaktu z centrum wsparcia IT Centralnego Ośrodka Informatyki:
• telefon + 48 (42) 253 54 50 czynny pn. – pt. w godzinach 7:00 – 18:00
• e-mail: epuap-pomoc@coi.gov.pl w sprawie ePUAP lub pz-pomoc@coi.gov.pl w sprawie profilu zaufanego.

z wyrazami szacunku,
Karol Okoński
Pełnomocnika Rządu ds. Cyberbezpieczeństwa
Sekretarz stanu
Ministerstwo Cyfryzacji
/-podpisano kwalifikowanym podpisem elektronicznym/

Pismo jest zgodne z wymaganiami WCAG 2.0 dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych, określonymi w załączniku nr 4 do 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. z 2017 poz. 2247)