„SUNRISE” P.H.U. Grzegorz Krzemieniecki
ul. A. Sacharowa 21/31
92-524 Łódź
tel. +602 710688, +512 232712
tel. / fax. +42 6734814
http://www.sunrise-phu.pl
e-mail: biuro@sunrise-phu.pl

Minister Cyfryzacji Marek Zagórski

ul. Królewska 27
00-060 Warszawa

WNIOSEK

O UDZIELENIE INFORMACJI PUBLICZNEJ

Działając na podstawie art. 61 Konstytucji wnoszę o udzielenie informacji publicznej w następującym zakresie:

1) **sposobu, okresu i procesu kontroli oraz weryfikacji stosowania się przez Stacje Kontroli Pojazdów do przepisów określonych jako „Wymogi Minimalne w Polityce Bezpieczeństwa Systemu Informatycznego Centralnej Ewidencji Pojazdów i Kierowców 2.0. Wymagania, zalecenia i wytyczne bezpieczeństwa dla Stacji Kontroli Pojazdów” wersja 1.00 z dnia 03.10.2017 r. obowiązujących od dnia 13 listopada 2017 r., w szczególności kontroli oraz weryfikacji wymagań, zaleceń i wytycznych zapisanych w punktach:**

5.3.1.1 - Zalecenia w zakresie konfiguracji urządzeń
- Użytkownicy łączący się z SI CEPiK 2.0 przez sieci dedykowane powinni przede wszystkim stosować się do wymagań i zaleceń określonych dla sieci dedykowanej, z której korzystają;
- Urządzenia sieciowe pozwalające na dostęp do sieci dedykowanej powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
  - administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności);
  - administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia;
  - zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC;

5.3.2.1 - Zalecenia w zakresie konfiguracji urządzeń i oprogramowania
- Urządzenia sieciowe pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich:
  - klucze prywatne do certyfikatów VPN zainstalowanych w urządzeniu musza być zabezpieczone w sposób uniemożliwiający dostęp do nich oraz ich wykorzystanie przez osoby nieuprawnione;
  - administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności);
  - administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia;

- zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC;
- zaleca się wdrożenie polityki blokowania dostępu do i z sieci publicznej Internet w czasie, w którym jest nawiązane połączenie VPN do SI CEPiK 2.0;
- oprogramowanie służące do zestawiania połączeń VPN typu Remote Access np. Cisco AnyConnect powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych do certyfikatów VPN osobom nieuprawnionym;

5.4.1.3 - Ochrona przed atakami zewnętrznymi (zapora ogniowa)
- Zalecane jest zastosowanie zapory ogniowej (rozwiązanie sprzętowe lub programowe) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację;

5.4.1.4 - Sieci Wi-Fi
- Do połączenia z sieciami Wi-Fi należy używać co najmniej standardu WPA i haseł o długości nie mniejszej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

5.4.1.5 - Ochrona antywirusowa
- Należy obowiązkowo stosować oprogramowanie antywirusowe oraz:
  - stosować ustawienia zapewniające aktualizację sygnatur antywirusowych na bieżąco lub
  - w przypadku braku dostępu do sygnatur antywirusowych na bieżąco, wdrożyć procedury zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu;

- Zalecana jest konfiguracja ustawień oprogramowania antywirusowego zapewniająca pełne skanowanie antywirusowe komputera:
  - co najmniej raz w tygodniu w przypadku braku aktualizacji sygnatur na bieżąco lub
  - co najmniej raz w miesiącu, w przypadku aktualizacji sygnatur na bieżąco;

- Konfiguracja oprogramowania antywirusowego ma wymuszać skanowanie każdego zewnętrznego nośnika danych (przenosiny dysk twardy, pamięć flasz) po jego podłączeniu do komputera;

5.4.1.8 - Dyski i urządzenia przenośne
- W przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach, powinny być one wyposażone w zamkniecie na kluczyk i zamknięte, gdy znajduje się w nich dysk. Po zakończonej pracy zalecane jest usuniecie dysku i jego dalsze przechowywanie w zabezpieczonej szafie;
- Należy wdrożyć regulacje zapewniające obsługę pamięci flasz oraz dysków przenośnych zawierających dane, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywać w bezpieczny sposób;
- Przenośne pamięci flasz oraz dyski przenośne, które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w rozwiązanie sprzętowe lub programowe umożliwiające szyfrowanie danych z użyciem hasła nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny);

5.4.1.10 - Kopie bezpieczeństwa
- Zalecane jest wdrożenie procedury tworzenia kopii zapasowych zapewniające wykonywanie kopii bezpieczeństwa nie rzadziej niż raz na 30 dni;

2) jakiemu podmiotowi zostanie powierzony nadzór i kontrola w sprawach określonych w pkt 1?

3) jakie wymagania powinien spełniać podmiot zajmujący się nadzorem i kontrolą w sprawach określonych w pkt 1?

4) **przywrócenia organizacji spotkań interesariuszy, w tym warsztatów legislacyjnych związanych z funkcjonowaniem CEP.**

Grzegorz Krzemieniecki

Łódź, dnia 13 sierpnia 2018 r.