RPW/6370/2021 P
Data:2021-02-04

Chełm, dnia 3 lutego 2021 r.

Egz. Nr 2.

WYSTĄPIENIE POKONTROLNE

Na podstawie § 4 i § 13 ust. 1 oraz § 8 ust. 1 załącznika do Decyzji Nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. *w sprawie wprowadzenia do stosowania Wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych* (Dz. Urz. MSW z 2012 r., poz. 43, z późn. zm.) zespół kontrolny przeprowadził w Wydziale Koordynacji Działań Nadbużańskiego Oddziału Straży Granicznej czynności kontrolne.

W związku z zakończeniem czynności kontrolnych w Wydziale Koordynacji Działań NOSG, stosownie do § 35 cytowanego powyżej aktu prawnego przekazuję Pani Naczelnik wystąpienie pokontrolne.

I. Nazwa i adres podmiotu kontrolowanego, imię i nazwisko kierownika podmiotu kontrolowanego:

Wydział Koordynacji Działań Nadbużańskiego Oddziału Straży Granicznej,
ul. Trubakowska 2, 22-100 Chełm,
ppłk SG Marta POGODA.

II. Imię, nazwisko i stanowisko służbowe kontrolerów:

Kierownik zespołu kontrolnego:

- mjr SG Dariusz GREGUŁA – kierownik Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 43/WOI/20 z dnia 03.09.2020 r.

Członkowie zespołu kontrolnego:

- mł. chor. SG Mariusz BIELAK – starszy specjalista – inspektor bezpieczeństwa teleinformatycznego Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 44/WOI/20 z dnia 03.09.2020 r.
- Paweł GRELA – specjalista – inspektor bezpieczeństwa teleinformatycznego Sekcji Ochrony Informacji Wydziału Ochrony Informacji Nadbużańskiego Oddziału Straży Granicznej – upoważnienie nr 45/WOI/20 z dnia 03.09.2020 r.

III. Data rozpoczęcia i zakończenia czynności kontrolnych:

Czynności kontrolne przeprowadzono w dniach 16, 17, 20 i 25 listopada 2020 r.

IV. Przedmiot kontroli:

Kontrola zgodności funkcjonowania akredytowanych systemów teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji:

1. System [redacted]
2. System
3. System
4. System
5. System

w szczególności:

a) zabezpieczenie globalnego i lokalnego środowiska bezpieczeństwa,
b) konfiguracji elektronicznego środowiska bezpieczeństwa,
c) dostępu użytkowników do systemu,
d) zgodności zainstalowanego oprogramowania z dokumentacją bezpieczeństwa,
e) aktualności dokumentacji bezpieczeństwa i dokumentacji pomocniczej.

V. Okres objęty kontrolą.

Stan bieżący.

VI. Ocena skontrolowanej działalności, ze wskazaniem ustaleń, na których została oparta:

Zespół kontrolny w trakcie przeprowadzonych czynności kontrolnych stwierdził co następuje:

1. System [redacted]
   – stanowisko nr [redacted].
2. System [redacted]:
   – stanowisko [redacted].
3. System [redacted]:
   – stanowisko [redacted].

Kontroli podlegały następujące zagadnienia umożliwiające ocenę działalności komórki kontrolowanej w zakresie:

1) *prawidłowości podłączenia (lub braku podłączenia) kontrolowanych stanowisk do sieci teleinformatycznej* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
2) *terminowego przeglądu okablowania przez lokalnych administratorów* – stwierdzono wpisy potwierdzające fakt dokonania przeglądu okablowania,
3) *zabezpieczenia stanowisk plombami* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

4) *rejestracji informatycznych nośników danych i materiałów wykorzystywanych w systemie* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

5) *prawidłowości konfiguracji ustawień BIOS* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

6) *prawidłowości konfiguracji systemu operacyjnego* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

7) *instalacji i konfiguracji oprogramowania antywirusowego* – stwierdzono zainstalowane oprogramowanie antywirusowe oraz jego poprawną konfigurację,

8) *aktualności oprogramowania antywirusowego* – stwierdzono termin aktualizacji zgodny z dokumentacjami bezpieczeństwa,

9) *zgodności zainstalowanego oprogramowania użytkowego z dokumentacją bezpieczeństwa* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

10) *założenia i usunięcia kont na podstawie Zleceń nadania/cofnięcia uprawnień* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

11) *zabezpieczeń globalnego i lokalnego środowiska bezpieczeństwa* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

12) *wyznaczenia osób funkcyjnych odpowiedzialnych za bezpieczeństwo systemu oraz posiadanie przez nich odpowiednich poświadczeń bezpieczeństwa i szkoleń oraz ważności poświadczeń bezpieczeństwa użytkowników oraz posiadanie przez nich odpowiednich szkoleń* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

13) *posiadania przez lokalnych administratorów podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z Procedurami Bezpiecznej Eksploatacji* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,

14) *aktualności prowadzenia „Dziennika działań administratora" przez lokalnych administratorów* – nie stwierdzono braku wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowisk,

15) *przeprowadzenia analizy logów systemowych przez lokalnych administratorów* – stwierdzono wpisy potwierdzające fakt przeprowadzenia analizy logów systemowych przez lokalnego administratora,

16) *aktualizacji „Załączników do SWB i PBE"* – nie stwierdzono błędnych lub nieaktualnych wpisów,

17) *posiadania przez lokalnych administratorów niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa.

W wyniku przeprowadzonych czynności kontrolnych zagadnień zawartych w pkt. od 1 do 17 nie stwierdzono nieprawidłowości w stosunku do kontrolowanych stanowisk systemów teleinformatycznych.

Stan funkcjonowania stanowisk systemów teleinformatycznych [redacted] oraz [redacted] wskazanych w części VI pkt. 1, 2 i 3 jest zgodny z dokumentacjami bezpieczeństwa.

W związku z powyższym kontrolowane zagadnienia należy ocenić pozytywnie.

4. System [redacted]
   – stanowisko [redacted].

5. System [redacted]
   – stanowisko [redacted].

Kontroli podlegały następujące zagadnienia umożliwiające ocenę działalności komórki kontrolowanej w zakresie:

1) *prawidłowości podłączenia (lub braku podłączenia) kontrolowanych stanowisk do sieci teleinformatycznej* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
2) *terminowego przeglądu okablowania przez lokalnego administratora* – stwierdzono wpisy potwierdzające fakt dokonania przeglądu okablowania,
3) *zabezpieczenia stanowisk plombami* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
4) *rejestracji informatycznych nośników danych i materiałów wykorzystywanych w systemie* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
5) *założenia i usunięcia kont na podstawie Zleceń nadania/cofnięcia uprawnień* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
6) *zabezpieczeń globalnego i lokalnego środowiska bezpieczeństwa* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
7) *wyznaczenia osób funkcyjnych odpowiedzialnych za bezpieczeństwo systemu oraz posiadanie przez nich odpowiednich poświadczeń bezpieczeństwa i szkoleń oraz ważności poświadczeń bezpieczeństwa użytkowników oraz posiadanie przez nich odpowiednich szkoleń* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
8) *posiadania przez lokalnego administratora podpisanych oświadczeń przez użytkowników systemu o zapoznaniu się z Procedurami Bezpiecznej Eksploatacji* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa,
9) *aktualności prowadzenia „Dziennika działań administratora" przez lokalnego administratora* – nie stwierdzono braku wpisów potwierdzających fakt wykonania prac administracyjnych lub związanych z bezpieczeństwem stanowisk,
10) *aktualizacji „Załączników do SWB i PBE"* – nie stwierdzono błędnych lub nieaktualnych wpisów,
11) *posiadania przez lokalnego administratora niezbędnej dokumentacji bezpieczeństwa oraz dokumentacji pomocniczej* – stwierdzono zgodność stanu faktycznego z dokumentacjami bezpieczeństwa.

W wyniku przeprowadzonych czynności kontrolnych zagadnień zawartych w pkt. od 1 do 11 nie stwierdzono nieprawidłowości w stosunku do kontrolowanych stanowisk systemów teleinformatycznych.

Stan funkcjonowania stanowisk systemów teleinformatycznych [redacted] oraz [redacted] wskazanych w części VI pkt. 4 i 5 jest zgodny z dokumentacjami bezpieczeństwa.

W związku z powyższym kontrolowane zagadnienia należy ocenić pozytywnie.

Reasumując, zespół kontrolny pozytywnie ocenia działalność Wydziału Koordynacji Działań NOSG w zakresie zgodności funkcjonowania akredytowanych systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych z przepisami szczególnych wymagań bezpieczeństwa i przestrzegania procedur bezpiecznej eksploatacji.

VII. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości:

W wyniku przeprowadzonej kontroli funkcjonowania akredytowanych systemów teleinformatycznych zespół kontrolny stwierdził, że zagadnienia podlegające kontroli były realizowane zgodnie z obwiązującymi przepisami.

W trakcie przeprowadzonych czynności kontrolnych nie ujawniono okoliczności wskazujących na popełnienie przestępstwa bądź wykroczenia.

Fakt przeprowadzenia przedmiotowej kontroli w trybie zwykłym odnotowano w Książce kontroli Komendy Nadbużańskiego Oddziału Straży Granicznej o nr. ewid. wg rejestru teczek nr NA-NK-1428/13, pod poz. 3/2020.

Podpis zarządzającego kontrolę:

KOMENDANT
Nadbużańskiego Oddziału Straży Granicznej
w Białej Podlaskiej

.....

Wykonano w 2 egz.:
Egz. Nr 1 – Wydział Koordynacji Działań NOSG
Egz. Nr 2 – a/a
Wykonał: zespół kontrolny, tel. 6655267
Dnia 02.02.2021 r.