MINISTER EDUKACJI NARODOWEJ

Warszawa, 11 kwietnia 2018 r.

BA-WA.0915.1.2017.MJ

Pan
Marek Charążka
Dyrektor
Centrum Informatycznego Edukacji

Wystąpienie pokontrolne

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz 1092) przedstawiam niniejsze Wystąpienie pokontrolne.

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. z 2011 r. Nr 185, poz. 1092) oraz art. 25 ust. 1 pkt 3 lit. b) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 j.t.) Ministerstwo Edukacji Narodowej[1], w okresie od dnia 13 czerwca do dnia 28 lipca 2017 r., przeprowadziło kontrolę w Centrum Informatycznym Edukacji (dalej: „Centrum" bądź „CIE") z siedzibą w Warszawie przy al. J. Ch. Szucha 25, w zakresie realizacji obowiązków utrzymania bezpieczeństwa teleinformatycznego w obszarze zapewnienia ciągłości działania, integralności oraz dostępności systemów i sieci teleinformatycznych działających na rzecz Ministerstwa Edukacji Narodowej.

Celem kontroli była ocena zapewnienia bezpieczeństwa teleinformatycznego systemów teleinformatycznych działających w MEN i obsługiwanych przez CIE. Kontrolą objęto okres od 24 listopada 2016 r. do 30 czerwca 2017 r.

CIE jest jednostką organizacyjną podległą Ministrowi Edukacji Narodowej.

W okresie objętym kontrolą przedmiot działalności CIE, zgodnie ze Statutem nadanym zarządzeniem nr 30 Ministra Edukacji Narodowej z dnia 25 października 2011 r., zmienionym zarządzeniem nr 6 Ministra Edukacji

---

[1] Kontrolę przeprowadzili pracownicy Ministerstwa Edukacji Narodowej:
1. Michał Jurkowski – naczelnik Wydziału Obsługi Administracyjnej Biura Administracyjnego, na podstawie upoważnienia nr 24/2017 z 13 czerwca 2017 r. – kierownik zespołu kontrolnego.
2. Paulina Lesiak – główny specjalista – Samodzielne Stanowisku do Spraw Obiegu Dokumentów w Postaci Elektronicznej w Biurze Organizacyjnym, na podstawie upoważnienia nr 25/2017 z 13 czerwca 2017 r.
3. Monika Bukowska-Łoś – Kierownik Samodzielnego Stanowiska do spraw Audytu Wewnętrznego, na podstawie upoważnienia nr 26/2017 z 13 czerwca 2017 r.

Narodowej z dnia 24 marca 2014 r. obejmował usługi informatyczne na rzecz Ministerstwa Edukacji Narodowej (§ 3 ust. 1 Statutu), tj. m.in.:

- projektowanie, programowanie, uruchamianie i utrzymywanie systemów informatycznych wspomagających zarządzanie,
- zapewnienie rozwoju i rozbudowy wdrażanych systemów informatycznych,
- utrzymywanie, rozwój i techniczną obsługę lokalnej sieci teleinformatycznej,
- zapewnienie dostępu do Internetu.

Obecnie obowiązujący Statut Centrum Informatycznego Edukacji, został nadany zarządzeniem nr 22 Ministra Edukacji Narodowej z dnia 21 czerwca 2017 r. Przedmiot działalności Centrum obejmuje usługi informatyczne na rzecz Ministerstwa Edukacji Narodowej (§ 3 ust. 1 Statutu), m.in.:

- projektowanie, programowanie, uruchamianie i utrzymywanie systemów informatycznych wspomagających zarządzanie i realizację zadań,
- zapewnienie rozwoju i rozbudowy utrzymywanych systemów informatycznych,
- zapewnienie bezpieczeństwa teleinformatycznego utrzymywanych systemów informatycznych,
- utrzymywanie oraz dbanie o wysoki standard infrastruktury informatycznej,
- zapewnienie dostępu do Internetu.

Działalność CIE w zakresie objętym kontrolą została oceniona pozytywnie. Ocenę uzasadniają ustalenia kontroli.

I. **Działania podejmowane przez CIE dla zapewnienia ciągłości działania:**
   a. **poczty elektronicznej,**
   b. **systemu Elektronicznego Zarządzania Dokumentami (EZD),**
   c. **Systemu Informacji Oświatowej (SIO),**
   d. **dostępu do usług Internetu.**

Centrum Informatyczne Edukacji, celem zapewnienia ciągłości działania systemów, dnia 4 września 2015 r. wprowadziło Procedurę Zarządzania Ciągłością Działania, w której zaplanowano reakcje na wypadek czasowych lub długotrwałych sytuacji kryzysowych, takich jak awarie systemów przetwarzania danych niezbędnych do realizacji działań statutowych, zminimalizowanie czasu trwania przerw oraz ewentualnych skutków ich wystąpienia przy zachowaniu bezpieczeństwa informacji. W ramach Procedury Zarządzania Ciągłością Działania dnia 24 lipca 2017 r., powołano: Sztab Kryzysowy, Zespół ds. Pierwszej Reakcji i Zespół ds. Infrastruktury i Systemów IT. Ponadto opracowano procedury awaryjne dotyczące utrzymania ciągłości działania: serwerów pocztowych, infrastruktury teleinformatycznej, w tym zapewnienia dostępu do usługi Internet, serwerów baz danych. W przypadku niezachowania

ciągłości dostarczania usług przez firmę świadczącą usługę hostingową, CIE opracowało również:

- plany odtworzeniowe opisujące przywrócenie utraconych plików oraz baz danych przez firmę świadczącą usługi hostingowe,
- plan utrzymania ciągłości działania Systemu Informacji Oświatowej,
- plan odtworzeniowy obejmujący przeniesienie działań krytycznych do lokalizacji zastępczej.

Raz do roku przeprowadzane są Testy Zarządzania Ciągłością Działania.

W celu zapewnienia bezpieczeństwa usług IT Centrum stosuje następujące środki ochrony:

a. dla poczty elektronicznej:
   - system antyspamowy w postaci klastra wirtualnych maszyn,
   - serwery pocztowe w postaci klastra wirtualnych maszyn,
   - kopie zapasowe systemu poczty elektronicznej,
   - okresowe przeprowadzanie testów odtworzeniowych danych z kopii zapasowych,
   - okresowe przeglądanie logów serwerów pocztowych i klastra wysokiej dostępności,
b. dla Systemu Elektronicznego Zarządzania Dokumentacją:
   - kopie zapasowe Systemu Elektronicznego Zarządzania Dokumentacją:
     - kopie w tle repozytorium plików wykonywane są co godzinę;
     - kopie zapasowe logów transakcyjnych bazy danych wykonywane są co godzinę;
     - pełne kopie zapasowe bazy danych wykonywane są codziennie;
     - przyrostowe kopie zapasowe serwerów (w tym repozytorium i bazy danych) wykonywane są codziennie;
     - pełne kopie zapasowe serwerów (w tym repozytorium i bazy danych) wykonywane są raz w tygodniu.

   Dla obu systemów wskazanych w pkt a. i b. CIE stosuje również poniższe środki ochrony:
   - monitorowanie podatności technicznych urządzeń oraz systemów IT,
   - monitorowanie wykorzystania zasobów sprzętowych, takich jak: obciążanie procesora, wykorzystanie pamięci operacyjnej, wykorzystania miejsca na dyskach,
   - aktualizowanie systemów,
   - stosowanie klastra wysokiej dostępności dla maszyn wirtualnych,
   - nadmiarowość[2] mająca na celu umożliwienie migracji maszyn wirtualnych w czasie awarii serwera fizycznego,
   - podtrzymanie awaryjne zasilania serwerów w postaci UPS'ów i agregatu prądotwórczego,
   - stosowanie Polityki Bezpieczeństwa Informacji.

[2] Nadmiarowość – jest to konfiguracja, która w momencie awarii serwera fizycznego, na którym są uruchomione maszyny wirtualne, pozwala na przeniesienie ich na inne zasoby.

c. dla Systemu Informacji Oświatowej:
- oprogramowanie raportujące o incydentach bezpieczeństwa występujących w systemie,
- Urządzenie UTM (wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia),
- Web Application Firewall,
- Loadbalancer (równoważenie obciążenia),
- serwer dystrybucji aktualizacji przeznaczonych dla systemów operacyjnych zainstalowany w infrastrukturze IT CIE,
- komputery wyposażone w oprogramowanie MS Windows, mające dostęp do serwerów systemu SIO, z zainstalowanym oprogramowaniem antywirusowym automatycznie aktualizowanym z wewnętrznego serwera aktualizacji,
- systemem wczesnego ostrzegania o zagrożeniach w sieci Internet będący efektem współpracy Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz działającego w ramach NASK zespołu CERT Polska.

d. w zakresie dostępu do usług Internetu:
- dwa niezależne łącza internetowe (światłowód, radiolinia),
- stosowanie klastra wysokiej dostępności dla przełączników sieciowych,
- aktualizowanie systemów,
- kopie zapasowe konfiguracji,
- Stosowanie Polityki Bezpieczeństwa Informacji.

W badanym zakresie nie stwierdzono nieprawidłowości.

II. Mechanizmy monitorowania integralności danych w bazie danych SIO.

Zgodnie z informacją przekazaną przez CIE, System Informacji Oświatowej jest systemem opartym o część centralną oraz oprogramowanie przeznaczone dla użytkowników końcowych systemu (baza lokalna[3]). CIE przyjęło następujące mechanizmy sprawdzające i zapewniające integralność i kompletność danych w bazie centralnej oraz bazie lokalnej:
- walidatory – mechanizmy sprawdzające poprawność wprowadzanych danych pod względem formatu (np. data) czy standardu (np. PESEL),
- weryfikacja – mechanizm sprawdzający czy wszystkie wymagane pola w formularzu zostały wprowadzone.

W bazie danych systemu centralnego oraz w bazach lokalnych wykorzystywane są standardowe mechanizmy zabezpieczające integralność danych tj.:

[3] Użytkownik końcowy systemu to osoba upoważniona do dostępu do aplikacji SIO. Na komputerze użytkownika po instalacji oprogramowania SIO jest tworzona lokalna baza danych, w której zapisywane są wszystkie wprowadzone przez użytkownika dane. Po ich zapisaniu do lokalnej bazy system automatycznie przekazuje je do części centralnej.

- klucze główne,
- klucze obce,
- „unique" (tzw. „wyjątkowości" służące do określania ograniczenia dla kolumny/kolumn w tabeli, dla której wartości nie mogą się powtarzać),
- słowniki.

W badanym zakresie nie stwierdzono nieprawidłowości.

III. Zabezpieczenie infrastruktury serwerowej, w tym serwera centralnego i serwera bazy danych SIO w zakresie utrzymania ciągłości działania.

Zabezpieczenie infrastruktury serwerowej, w tym serwera bazy danych SIO i serwera centralnego zostało wymienione w pkt I lit. c. Przy określaniu poziomu i sposobu zabezpieczenia infrastruktury serwerowej, Centrum uwzględnia także poniższe czynniki oraz sposoby konfiguracji i użytkowania infrastruktury IT SIO:

- ilość możliwych zagrożeń dla środowisk linux – określona jako znikoma,
- serwery działające w oparciu o systemy łączące się z zewnętrznymi serwerami dystrybucji aktualizacji – wprowadzono centralny serwer dystrybucji aktualizacji,
- niedostępne publicznie serwery dedykowane systemowi SIO,
- infrastruktura IT chroniona przez urządzenie UTM,

Infrastruktura informatyczna będąca w zarządzaniu CIE jest także okresowo poddawana testom penetracyjnym przez CERT Polska. Inicjatorem przeprowadzania testów jest Centrum, które uzgadnia możliwość ich przeprowadzenia z CERT Polska. Testy te stanowią podstawę do optymalizacji konfiguracji zabezpieczeń infrastruktury IT CIE.

W badanym zakresie nie stwierdzono nieprawidłowości.

IV. Narzędzia wprowadzone dla ochrony przed fizyczną ingerencją w infrastrukturę IT.

Centrum wprowadziło następujące rozwiązania służące ochronie przed fizyczną ingerencją w infrastrukturę IT:

a) System Kontroli Dostępu.
Infrastruktura IT jest fizycznie chroniona poprzez funkcjonujący w budynku MEN System Kontroli Dostępu. Pomieszczenia, w których znajduje się kluczowa infrastruktura IT (np. serwerownia) są zabezpieczone poprzez zainstalowane czytniki kart zbliżeniowych lub zamki, które uniemożliwiają dostęp osobom trzecim. Dostęp osób do chronionych pomieszczeń jest związany z realizowanymi przez nie zadaniami. Uprawnienia dostępu do tych pomieszczeń są wydawane przez wyznaczonych pracowników CIE. Ochronę stanowi system „Klucze", dzięki któremu dostęp do poszczególnych kluczy i pomieszczeń mają osoby wyłącznie do tego uprawnione. Ochroną, poprzez system alarmowy i kamery, objęty jest również magazyn sprzętu komputerowego. Pomieszczenie serwerowni

wyposażone jest ponadto w system klimatyzacji, detekcji pożaru oraz system automatycznego gaszenia.

b) Monitoring wizyjny.
Budynek MEN posiada oznaczenia „OBIEKT MONITOROWANY". Zabezpieczenie budynku poprzez monitoring wizyjny pozwala śledzić pracownikom ochrony zarówno bezpośrednie otoczenie budynku, jak i wytypowane fragmenty wewnątrz obiektu. System pozwala na bieżącą obserwację obszarów oraz, dzięki rejestrowaniu obrazu, umożliwia przeglądanie wsteczne.

c) Ochrona fizyczna.
Budynek jest chroniony przez pracowników firmy ochroniarskiej, która sprawuje nadzór nad ruchem osób, przedmiotów w budynku oraz pojazdów w jego bezpośrednim otoczeniu. Posiadanie identyfikatora umożliwia wejście do budynku.

W badanym zakresie nie stwierdzono nieprawidłowości.

V. Sposób ochrony sieci Wi-Fi.

Centrum zapewnia Ministerstwu Edukacji Narodowej jedną otwartą sieć WiFi oraz dwie sieci WiFi wymagające podania hasła (szyfrowanie WPA2). Wszystkie sieci WiFi odizolowane są od sieci LAN przy użyciu VLAN oraz posiadają włączoną izolację klientów. Izolacja klientów uniemożliwia komunikację klientów WiFi pomiędzy sobą. Dostęp klientów do Internetu wykonywany jest wyłączenie po protokołach http, https.

W badanym zakresie nie stwierdzono nieprawidłowości.

VI. Rejestr incydentów naruszenia bezpieczeństwa informacji wraz z zapisami reakcji na incydenty.

Zgodnie z Procedurą Zarządzania Incydentami, CIE raz na pół roku sporządza raport incydentów bezpieczeństwa informacji. W drugim półroczu 2016 r. zgłoszono 3 incydenty, a w pierwszym półroczu 2017 r. 5 incydentów naruszenia bezpieczeństwa informacji.

Wszystkie przypadki zgłoszonych incydentów zostały objęte działaniami, które skupiły się na przywróceniu poprawnego funkcjonowania systemów poprzez identyfikację luk, błędów w systemach oraz ich usunięciu przez serwisantów i konserwatorów systemu.

Mając na względzie podjęte, po stwierdzonych incydentach, działania zaradcze, w badanym zakresie nie stwierdzono nieprawidłowości.

VII. Informacje w zakresie zagrożeń bezpieczeństwa teleinformatycznego zgłaszane przez CERT lub inne instytucje państwowe.

Wymiana informacji pomiędzy CIE a CERT Polska odbywa się za pomocą dwóch kanałów komunikacji. Pierwszym kanałem komunikacji są pisma i dokumenty papierowe, natomiast drugim jest poczta elektroniczna. CIE wskazało administratorów technicznych odpowiedzialnych za kontakt z CERT Polska. W okresie od 24 listopada 2016 r. do 30 czerwca 2017 r. CERT Polska przekazało ustandaryzowane informacje o potencjalnych zagrożeniach bezpieczeństwa dla jednostek administracji publicznej i stosowne zalecane działania. Powyższe zalecenia zostały przez CIE wdrożone (m.in. blokada wskazanych przez CERT Polska adresów IP oraz domen).

W badanym zakresie nie stwierdzono nieprawidłowości.

VIII. Aktualizacja systemów operacyjnych oraz oprogramowania antywirusowego na stacjach roboczych pracowników MEN.

Aktualizacja systemów operacyjnych Windows odbywa się codziennie. System antywirusowy weryfikuje serwer na stacjach klienckich pod kątem aktualności sygnatur. CIE prowadzi wykaz stacji roboczych pracowników MEN, dla których cykliczna aktualizacja systemów operacyjnych oraz oprogramowania antywirusowego skończyła się niepowodzeniem. Wykaz ten jest na bieżąco aktualizowany. W przypadku problemów z aktualizacją zostaje podjęta, przez pracowników CIE, próba bezpośredniej naprawy na stacji roboczej. Na komputerach przenośnych aktualizacje definicji wirusów oprogramowania antywirusowego pobierane są automatycznie z serwerów dostawcy oprogramowania. Proces pobierania i instalacji aktualizacji systemów operacyjnych przebiega automatycznie – warunkiem jest podłączenie komputera do sieci LAN w budynku MEN lub połączenie poprzez sieć VPN.

W badanym zakresie nie stwierdzono nieprawidłowości.

IX. System antyspamowy i antywirusowy dla poczty elektronicznej.

CIE użytkuje system antyspamowy w postaci klastra wirtualnych maszyn, który jest aktualizowany na bieżąco (baza wirusów i spamu), co oznacza, że w przypadku wydania nowej sygnatury jest ona pobierana do systemu.

W badanym zakresie nie stwierdzono nieprawidłowości.

X. Wyniki ostatniego auditu wewnętrznego w zakresie funkcjonowania w CIE Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI).

W terminie od 16 do 18 maja 2017 r. w Centrum został przeprowadzony audit wewnętrzny SZBI sprawdzający skuteczność wdrożenia dokumentacji SZBI w CIE. W wyniku przeprowadzonego auditu zalecono:

- uzupełnienie ofert firm biorących udział w zapytaniu ofertowym),
- aktualizację listy osób zespołu ds. pierwszej reakcji,
- aktualizację listy osób ze sztabu kryzysowego.

Wskazane zalecenia zostały wykonane. Mając na względzie wdrożone przez CIE mechanizmy korygujące i zapobiegawcze, nie stwierdzono nieprawidłowości w badanym zakresie.

XI. Zasady przeprowadzania inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji.

W CIE inwentaryzacja sprzętu IT i oprogramowania przeprowadzana jest na podstawie zarządzenia dyrektora CIE w trybie spisu z natury, w okresach wynikających z ustawy o rachunkowości. Ostatnia inwentaryzacja całego majątku została przeprowadzona w 2016 r. wg stanu na 31 października 2016 r. zgodnie z zarządzeniem nr 15/2016 Dyrektora Centrum Informatycznego Edukacji z 6 października 2016 r. w sprawie przeprowadzenia inwentaryzacji okresowej składników majątkowych Centrum Informatycznego Edukacji. W celu realizacji procesu gospodarowania majątkiem zostały powołane stałe komisje oceny przydatności do dalszego użytkowania i likwidacji składników rzeczowych majątku ruchomego oraz praw na dobrach niematerialnych.

W badanym zakresie nie stwierdzono nieprawidłowości.

XII. Sposób nadawania przez CIE uprawnień do pracy w systemach informatycznych.

Zgodnie z Procedurą Administrowania Systemami Informatycznymi z dnia 1 września 2014 r. każde nadanie, modyfikacja i odbieranie uprawnień do systemów informatycznych dla pracownika odbywa się na wniosek jego przełożonego. Wniosek o nadanie, zmianę lub odebranie dostępu do zasobów podlega akceptacji Właściciela zasobu, o ile nie jest nim sam wnioskujący. Po akceptacji wniosku przez Właściciela zasobu, przekazywany jest on do właściwego Administratora Systemu Informatycznego do akceptacji i nadania, modyfikacji lub odebrania uprawnień przez właściwego Administratora Technicznego. W przypadku braku akceptacji, Właściciel zasobu powiadamia wnioskującego o odrzuceniu wniosku i przyczynie odrzucenia. Spory w kwestii nadania/odebrania uprawnień rozstrzyga Dyrektor CIE, bądź osoba przez niego upoważniona.

W badanym zakresie nie stwierdzono nieprawidłowości.

XIII. Program szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji, uwzgledniający tematy zagrożeń w zakresie bezpieczeństwa informacji i zabezpieczeń w tym obszarze.

Wdrożony w CIE program szkoleń z dnia 26 października 2015 r. przewiduje szkolenie w zakresie bezpieczeństwa informacji dla każdego

nowozatrudnionego pracownika, który zaangażowany jest w proces przetwarzania informacji. Szkolenie, w formie prezentacji, przeprowadza Pełnomocnik ds. SZBI. W II półroczu 2016 r. przeprowadzono 3 szkolenia, natomiast w I półroczu 2017 r. 6 szkoleń.
Administratorzy systemów informatycznych w CIE na bieżąco aktualizują swoją wiedzę o zagrożeniach informatycznych wykorzystując specjalistyczne portale internetowe oraz czasopisma branżowe. W badanym zakresie nie stwierdzono nieprawidłowości.

XIV. Działania zapewniające ciągłość działania Systemu Elektronicznego Zarządzania Dokumentacją (EZD) Ministerstwa Edukacji Narodowej.

W przypadku wystąpienia błędów w działaniu Systemu Elektronicznego Zarządzania Dokumentacją zgłaszanych bezpośrednio przez użytkowników do CIE, administratorzy techniczni konsultują się z administratorem merytorycznym w MEN w celu potwierdzenia, czy zgłoszona awaria dotyczy całego systemu czy występuje tylko lokalnie. Jeżeli jest to problem lokalny, związany z działaniem sprzętu komputerowego rozwiązaniem problemu zajmuje się Sekcja Wsparcia Użytkownika w CIE. Natomiast, jeżeli jest to problem lokalny związany z kwestiami merytorycznymi, rozwiązaniem problemu zajmują się administratorzy merytoryczni w MEN.

W przypadku awarii zgłaszanej przez administratorów merytorycznych do Centrum, diagnozowana jest przyczyna wystąpienia błędu i możliwości naprawy. Weryfikowane jest także prawidłowe działanie usług na serwerach EZD. Jeżeli problem wystąpił po raz pierwszy weryfikowane jest jego występowanie w środowisku testowym. Natomiast w sytuacji, kiedy problem występuje zarówno w środowisku testowym, jak i produkcyjnym systemu i wynika on z błędu aplikacji, zgłoszenie jest kierowane do dostawcy oprogramowania, tj. Podlaskiego Urzędu Wojewódzkiego (PUW) w celu jego wyeliminowania.

CIE ma możliwość odtworzenia danych z systemu EZD z przechowywanych kopii zapasowych. Na serwerach Systemu EZD uruchomiono mechanizm monitorowania wykorzystania pojemności dysków twardych, który wysyła powiadomienia do administratorów technicznych systemu w przypadku przekroczenia założonych wartości.

Administratorzy techniczni systemu EZD prowadzą dziennik administratora systemu w formie elektronicznej. W dzienniku odnotowywane są wszelkie istotne techniczne zmiany, mające lub mogące mieć wpływ na działanie systemu EZD, ze szczególnym uwzględnieniem zmian dokonywanych przez administratorów w bazie danych systemu (np. zmiana konfiguracji, aktualizacja, modyfikacja sprzętu, obsługa incydentów itd.).

W badanym zakresie nie stwierdzono nieprawidłowości.

Z upoważnienia
MINISTRA EDUKACJI NARODOWEJ

DYREKTOR GENERALNY
Joanna Szczawińska