



DZIENNIK URZĘDOWY

AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

Warszawa, dnia 15 października 2014 r.

Poz. 18

ZARZĄDZENIE NR 26 SZEFA AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

z dnia 5 czerwca 2014 r.

w sprawie powołania Zespołu Reagowania na Incydenty Komputerowe CERT - ABW

Na podstawie art. 20 ust. 4 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.¹⁾), zarządza się, co następuje:

Rozdział 1. Przepisy ogólne

§ 1. Zarządzenie określa:

- 1) zakres zadań Zespołu Reagowania na Incydenty Komputerowe CERT - ABW, zwanego dalej „CERT - ABW”;
- 2) organizację oraz skład CERT - ABW;
- 3) zasady funkcjonowania CERT - ABW;
- 4) sposób zgłaszania incydentów bezpieczeństwa teleinformatycznego oraz podatności do CERT - ABW;
- 5) zasady oraz tryb sporządzania oraz przekazywania raportów z pracy CERT - ABW;
- 6) tryb współdziałania CERT - ABW z jednostkami organizacyjnymi Agencji Bezpieczeństwa Wewnętrznego, zwanej dalej „ABW”.

§ 2. Użyte w zarządzeniu określenia oznaczają:

- 1) „system teleinformatyczny” - system, o którym mowa w art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422);
- 2) „incydent bezpieczeństwa teleinformatycznego” - zdarzenie lub seria zdarzeń, które mogą obniżać poziom bezpieczeństwa systemów teleinformatycznych oraz przetwarzanych w nich informacji, w szczególności wpływając na ich poufność, integralność oraz dostępność;
- 3) „podatność systemu teleinformatycznego” - właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie.

Rozdział 2. Powołanie CERT - ABW

§ 3. 1. Tworzy się CERT - ABW, jako wewnętrzny zespół o charakterze stałym, realizujący zadania z obszaru zapewniania oraz podwyższania bezpieczeństwa jawnych systemów teleinformatycznych, których właścicielem jest ABW.

¹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2010 r. Nr 182, poz. 1228 i Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273, Nr 84, poz. 455, Nr 117, poz. 677 i Nr 230, poz. 1371, z 2012 r. poz. 627 i 908, z 2013 r. poz. 628, 675, 1247 i 1351 oraz z 2014 r. poz. 502 i 544.

2. Właściwość rzeczowa CERT - ABW nie obejmuje systemów teleinformatycznych wykorzystywanych przez Rządowy Zespół Reagowania na Incydeny Komputerowe CERT.GOV.PL.

Rozdział 3. Zakres zadań CERT - ABW

§ 4. 1. Do szczegółowych zadań CERT - ABW należy:

- 1) reagowanie na incydeny bezpieczeństwa teleinformatycznego oraz wykryte podatności, występujące w jawnych systemach teleinformatycznych, których właścicielem jest ABW;
- 2) obsługa i analiza incydentów bezpieczeństwa teleinformatycznego oraz podatności, o których mowa w pkt 1;
- 3) nie rzadziej niż raz w roku analiza poziomu bezpieczeństwa jawnych systemów teleinformatycznych, których właścicielem jest ABW oraz możliwości poprawy stanu ich bezpieczeństwa;
- 4) publikacja powiadomień oraz ostrzeżeń z zakresu bezpieczeństwa teleinformatycznego, realizowana w szczególności za pośrednictwem intranetowej strony ABW;
- 5) sporządzanie oraz przekazywanie Dyrektorowi Departamentu Bezpieczeństwa Teleinformatycznego ABW, zwanego dalej „Departamentem I”, rocznych raportów z działalności zawierających ramowe plany działań na kolejny rok;
- 6) organizowanie oraz współorganizowanie szkoleń z zakresu bezpieczeństwa teleinformatycznego dla funkcjonariuszy oraz pracowników ABW.

2. Czynności kontrolne podejmowane na podstawie informacji uzyskanych w ramach funkcjonowania CERT - ABW, prowadzone są na podstawie przepisów odrębnych.

3. Jednostką organizacyjną ABW właściwą do prowadzenia kontroli, o której mowa w ust. 2, jest Departament Bezpieczeństwa Wewnętrznego i Audytu ABW, zwany dalej „Departamentem VI”.

4. W szczególnie uzasadnionych przypadkach, na polecenie Dyrektora Departamentu I ABW po uzyskaniu zgody Szefa ABW, CERT - ABW ma prawo do przeprowadzania testów bezpieczeństwa jawnych systemów teleinformatycznych, których właścicielem jest ABW.

5. Testy bezpieczeństwa, o których mowa w ust. 4, przeprowadzane są z zachowaniem właściwości rzeczowej we współpracy z Departamentem VI ABW oraz jednostkami organizacyjnymi ABW, które wykorzystują atestowane systemy.

Rozdział 4. Organizacja oraz skład CERT - ABW

§ 5. 1. Zespołem CERT - ABW kieruje naczelnik Wydziału III Departamentu I ABW, zwany dalej „Kierownikiem CERT - ABW”.

2. Wsparcie organizacyjne CERT - ABW zapewnia Wydział III Departamentu I ABW.

3. W skład CERT - ABW wchodzi:

- 1) naczelnik Wydziału II Departamentu I ABW - pełniący rolę zastępcy Kierownika CERT - ABW;
- 2) naczelnik Wydziału V Departamentu I ABW;
- 3) naczelnik Wydziału IX Departamentu I ABW;
- 4) sześciu funkcjonariuszy Departamentu I ABW wyznaczonych przez Dyrektora Departamentu I ABW.

4. W przypadku czasowej nieobecności w CERT - ABW naczelników, o których mowa w ust. 3 pkt 1-3, zadania w CERT - ABW przejmują ich zastępcy.

5. W uzasadnionych przypadkach, Kierownik CERT - ABW może występować do właściwych przełożonych o włączenie do konkretnych czynności podejmowanych przez CERT - ABW także innych funkcjonariuszy Departamentu I ABW oraz funkcjonariuszy samodzielnych sekcji Bezpieczeństwa Teleinformatycznego, zgodnie z właściwością terytorialną delegatury ABW.

6. Na polecenie Dyrektora Departamentu I ABW w skład CERT - ABW mogą tymczasowo wchodzić dodatkowi funkcjonariusze Departamentu I ABW oraz, w porozumieniu z Dyrektorem Departamentu VI ABW, funkcjonariusze Departamentu VI ABW.

7. Za zgodą bezpośrednich przełożonych, w skład CERT - ABW mogą być włączani również funkcjonariusze innych jednostek organizacyjnych ABW.

Rozdział 5. Zasady funkcjonowania CERT - ABW

§ 6. 1. CERT - ABW przyjmuje zgłoszenia wystąpienia incydentów bezpieczeństwa teleinformatycznego lub podatności na zasadach, o których mowa w § 7.

2. Nadzór merytoryczny nad działalnością CERT - ABW pełni Dyrektor Departamentu I ABW.

3. Za realizację zadań CERT - ABW odpowiada Kierownik CERT - ABW.

4. Do zadań Kierownika CERT - ABW należy:

- 1) organizowanie pracy CERT - ABW;
- 2) określanie aktualnych kierunków działań CERT - ABW oraz ustalanie ich priorytetów;
- 3) określanie zakresu zadań realizowanych przez poszczególnych członków CERT - ABW z uwzględnieniem przepisów odrębnych;
- 4) przydzielanie prac członkom CERT - ABW, zgodnie z ich zakresem zadań;
- 5) zwoływanie spotkań roboczych lub posiedzeń CERT - ABW;
- 6) przedstawianie Dyrektorowi Departamentu I ABW rocznego raportu z pracy CERT - ABW.

5. W terminie do końca I kwartału każdego roku kalendarzowego, CERT - ABW sporządza raport roczny z funkcjonowania CERT - ABW w roku poprzednim. Raport zawiera w szczególności:

- 1) podsumowanie prac - w tym statystyki wykrytych incydentów bezpieczeństwa teleinformatycznego lub podatności oraz opis podjętych działań;
- 2) analizę bezpieczeństwa jawnych systemów teleinformatycznych, których właścicielem jest ABW;
- 3) wnioski odnoszące się do przyszłych działań, mających na celu podwyższenie poziomu bezpieczeństwa systemów teleinformatycznych.

6. Roczny raport przedkładany jest przez Kierownika CERT - ABW Dyrektorowi Departamentu I ABW oraz Departamentu VI ABW.

Rozdział 6. Sposób zgłaszania incydentów bezpieczeństwa teleinformatycznego oraz podatności

§ 7. 1. Użytkownicy systemów teleinformatycznych ABW zgłaszają do CERT - ABW informacje o możliwości wystąpienia incydentu bezpieczeństwa teleinformatycznego lub podatności systemu, za pośrednictwem formularza zamieszczonego w wewnętrznej sieci teleinformatycznej ABWAN <http://incydenty.warszawa.abw.waw/>.

2. Zgłoszenie powinno zawierać opis wszelkich nieprawidłowości lub podejrzanych działań występujących w systemie teleinformatycznym.

3. CERT - ABW uprawniony jest do kierowania zapytań uzupełniających zgłoszenia, o których mowa w ust. 1.

Rozdział 7. Współpraca CERT - ABW z jednostkami organizacyjnymi ABW

§ 8. 1. W uzasadnionych przypadkach, Kierownik CERT - ABW z zachowaniem drogi służbowej, może występować do kierowników jednostek organizacyjnych ABW z wnioskiem o podjęcie wspólnych działań lub udzielenie pomocy.

2. Wnioski o współpracę z CERT - ABW, w tym dotyczące organizacji bądź prowadzenia prezentacji lub szkoleń, kierownicy jednostek organizacyjnych ABW kierują do Dyrektora Departamentu I ABW.

Rozdział 8.
Przepisy przejściowe i końcowe

§ 9. Sprawy związane z obsługą i zgłaszaniem incydentów bezpieczeństwa teleinformatycznego występujących w jawnych systemach teleinformatycznych, których właścicielem jest ABW, pozostających we właściwości Departamentu I ABW, przechodzą do zadań CERT - ABW.

§ 10. Przepisy niniejszego zarządzenia stosuje się do spraw wszczętych i niezakończonych przed dniem jego wejścia w życie.

§ 11. Zarządzenie wchodzi w życie z dniem podpisania.

Szef
Agencji Bezpieczeństwa Wewnętrznego

plk Dariusz ŁUCZAK