Warszawa, dnia 23 czerwca 2014 r.
Poz. 203

Narodowe Centrum Kryptologii

DECYZJA Nr 243 /MON
MINISTRA OBRONY NARODOWEJ

z dnia 18 czerwca 2014 r.

w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej

Na podstawie art. 2 pkt 6a ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2013 r. poz. 189 i 852) oraz § 1 pkt 1 lit. a i d, pkt 2 lit. e i § 2 pkt 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w związku z § 5 ust. 2 pkt 3 regulaminu organizacyjnego Ministerstwa Obrony Narodowej, stanowiącego załącznik do zarządzenia Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej (Dz. Urz. Min. Obr. Nar. Nr 21, poz. 270, z późn. zm.[1)]), ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:
   1) administrator systemu teleinformatycznego – osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie jawnego lub niejawnego systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego;

[1)] Zmiany wymienionego zarządzenia zostały ogłoszone w Dz. Urz. Min. Obr. Nar. z 2007 r. Nr 4, poz. 38, Nr 6, poz. 73, Nr 17, poz. 176 i Nr 21, poz. 209, z 2008 r. Nr 8, poz. 85, Nr 15, poz. 188, Nr 20, poz. 260 i Nr 23, poz. 287, z 2009 r. Nr 2, poz. 17, z 2010 r. Nr 10, poz. 106 i Nr 23, poz. 304, z 2011 r. Nr 5, poz. 54, z 2012 r. poz. 106, 307, 313 i 363, z 2013 r. poz. 157, 231 i 356 oraz z 2014 r. poz. 88.

2) incydent bezpieczeństwa teleinformatycznego – pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji, które zagrażają ich poufności, dostępności lub integralności;
3) incydent komputerowy – pojedyncze zdarzenie lub seria zdarzeń dotyczących sprzętu komputerowego lub jego oprogramowania, stanowiących część incydentu bezpieczeństwa teleinformatycznego;
4) jednostka organizacyjna – Ministerstwo Obrony Narodowej oraz jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
5) komórka organizacyjna – komórkę organizacyjną Ministerstwa Obrony Narodowej w rozumieniu § 2 pkt 5 regulaminu organizacyjnego Ministerstwa Obrony Narodowej, stanowiącego załącznik do zarządzenia Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej;
6) kierownik jednostki (komórki) organizacyjnej – dowódcę, szefa, dyrektora, komendanta lub inną osobę kierującą działalnością jednostki lub komórki organizacyjnej, w tym osobę czasowo pełniącą obowiązki;
7) organizator systemu teleinformatycznego – kierownika jednostki organizacyjnej organizującej system teleinformatyczny lub upoważnionego przez niego kierownika komórki organizacyjnej;
8) pełnomocnik ochrony – pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych;
9) reagowanie – zachowanie lub postępowanie, jako odpowiedź na zaistniałe zdarzenie;
10) SRnIK – System Reagowania na Incydenty Komputerowe resortu obrony narodowej zorganizowany w trzypoziomową strukturę, w skład, której wchodzą:
    a) Centrum Koordynacyjne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Narodowego Centrum Kryptologii,
    b) Centrum Techniczne SRnIK, którego funkcję spełnia właściwa komórka wewnętrzna Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych,
    c) administratorzy systemów teleinformatycznych w jednostkach i komórkach organizacyjnych;
11) system teleinformatyczny – system teleinformatyczny w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów

realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235 oraz z 2014 r. poz. 183);

12) zagrożenie – potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;

13) dokumentacja bezpieczeństwa teleinformatycznego – dokumentację w rozumieniu § 25 i 26 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948);

14) zdarzenie – zmiana stanu systemu lub usługi, która wskazuje na możliwe naruszenie polityki bezpieczeństwa lub procedur zawartych w dokumentacji bezpieczeństwa teleinformatycznego, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

15) inspektor bezpieczeństwa teleinformatycznego – osobę lub zespół osób wyznaczonych do realizacji zadań w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego przetwarzającego informacje niejawne z jego dokumentacją bezpieczeństwa teleinformatycznego;

16) cyberprzestrzeń – cyberprzestrzeń w rozumieniu art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. Nr 156 poz. 1301, z późn. zm.[2)]).

2. SRnIK organizuje się w celu zapewnienia koordynacji i realizacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach teleinformatycznych oraz autonomicznych stanowiskach komputerowych resortu obrony narodowej, z wyłączeniem systemów teleinformatycznych i narodowych segmentów międzynarodowych systemów teleinformatycznych Służby Wywiadu Wojskowego oraz Służby Kontrwywiadu Wojskowego, a także systemów Żandarmerii Wojskowej wykorzystywanych bezpośrednio do prowadzenia działalności dochodzeniowo-śledczej oraz operacyjno-rozpoznawczej.

3. Nadzór nad funkcjonowaniem SRnIK sprawuje Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.

4. Centrum Koordynacyjne SRnIK:

1) określa ogólne zasady funkcjonowania SRnIK;

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 228, poz. 2261, z 2004 r. Nr 107, poz. 1135, z 2011 r. Nr 222, poz. 1323 oraz z 2014 r. poz. 498.

2) współpracuje w zakresie ustalania formalno-prawnych zasad funkcjonowania SRnIK oraz planów jego rozwoju w wymiarze krajowym i międzynarodowym z:
   a) Służbą Kontrwywiadu Wojskowego,
   b) Żandarmerią Wojskową,
   c) Departamentem Ochrony Informacji Niejawnych,
   d) Organizatorem Systemu Funkcjonalnego Wsparcia Dowodzenia,
   e) Centrum Technicznym SRnIK w zakresie ustalania ogólnych zasad funkcjonowania SRnIK,
   f) Centrum Koordynacyjnym systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
   g) krajowymi i międzynarodowymi organami koordynującymi systemy reagowania na incydenty komputerowe;
3) realizuje zadania wynikające z Planu Zarządzania Kryzysowego MON, Wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planu Operacyjnego Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny;
4) bierze udział w pracach grup roboczych w ramach Organizacji Traktatu Północnoatlantyckiego oraz reprezentuje resort obrony narodowej w kontaktach z organizacjami spoza resortu obrony narodowej, w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych;
5) prowadzi ewidencję systemów teleinformatycznych objętych SRnIK, na podstawie danych otrzymanych od organizatorów systemów teleinformatycznych.

5. Centrum Techniczne SRnIK:
   1) współpracuje z Centrum Koordynacyjnym SRnIK w zakresie ustalania ogólnych zasad funkcjonowania SRnIK;
   2) prowadzi działania polegające na wydawaniu biuletynów informacyjnych, analizie infrastruktury teleinformatycznej, opracowywaniu zaleceń i wytycznych zapobiegających wystąpieniu incydentów komputerowych;
   3) współpracuje w zakresie reagowania na incydenty komputerowe i incydenty bezpieczeństwa teleinformatycznego z:
      a) Rządowym Zespołem Reagowania na Incydenty Komputerowe,
      b) Służbą Kontrwywiadu Wojskowego,
      c) właściwymi pionami ochrony informacji niejawnych,

d) Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania przestępstw komputerowych – w zakresie bezpieczeństwa systemów teleinformatycznych w resorcie obrony narodowej oraz reagowania na podejrzenie popełnienia przestępstwa przeciwko ochronie informacji,
e) Rządowym Centrum Bezpieczeństwa,
f) Dowództwem Operacyjnym Rodzajów Sił Zbrojnych,
g) Centrum Technicznym systemu reagowania na incydenty komputerowe Organizacji Traktatu Północnoatlantyckiego,
h) krajowymi i międzynarodowymi zespołami systemu reagowania na incydenty komputerowe,
i) organizatorami systemów teleinformatycznych,
j) kierownikami jednostek organizacyjnych i komórek organizacyjnych poprzez administratorów systemów teleinformatycznych;

4) monitoruje stan bezpieczeństwa nadzorowanych systemów teleinformatycznych;
5) realizuje zadania związane z bezpośrednią obsługą incydentów komputerowych w systemach teleinformatycznych według odpowiednich procedur;
6) prowadzi wykaz osób funkcyjnych odpowiedzialnych za SRnIK, w tym danych teleadresowych;
7) zbiera i analizuje informacje o zdarzeniach oraz tworzy na ich bazie okresowe raporty o stanie bezpieczeństwa w systemach teleinformatycznych dla potrzeb organizatorów systemów, Centrum Koordynacyjnego SRnIK oraz Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni;
8) organizuje dla personelu komórek i jednostek organizacyjnych szkolenia z zakresów reagowania na incydenty komputerowe oraz bezpieczeństwa teleinformatycznego;
9) stosuje, uzgodnione z organizatorem systemu oraz Pełnomocnikiem Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, środki techniczne i organizacyjne oraz narzędzia do zdalnego zarządzania i kontroli konfiguracji systemów teleinformatycznych, służące do zapobiegania, wykrywania i usuwania skutków incydentów komputerowych. W przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, zastosowanie wyżej wymienionych rozwiązań uwzględnia się w szacowaniu ryzyka oraz dokumentacji bezpieczeństwa systemu

teleinformatycznego. W powyższym zakresie organizator systemu uzgadnia dokumentację bezpieczeństwa z Centrum Technicznym SRnIK;

10) realizuje, na polecenie Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, wniosek organizatora systemu lub organu akredytującego, w porozumieniu z organizatorem systemu, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych również z właściwym pionem ochrony, za wiedzą organizatora i organu akredytującego, testy bezpieczeństwa i testy podatnościowe, mające na celu weryfikację poprawności funkcjonowania zabezpieczeń, ustalenie ich aktualnego stanu oraz rekomendowanie skutecznych rozwiązań;
11) prowadzi portale informacyjne w sieci INTER-MON i MIL-WAN na potrzeby obsługi incydentów komputerowych i prowadzonych działań informacyjnych;
12) wnioskuje do organizatora systemu w sprawie czasowego wyłączania lub zaniechania przetwarzania informacji w systemie lub części systemu teleinformatycznego przetwarzającego informacje niejawne, w której stwierdzono wystąpienie incydentu komputerowego;
13) podejmuje decyzje o czasowym odłączeniu systemu teleinformatycznego posiadającego połączenie z siecią Internet, w którym stwierdzono wystąpienie incydentu komputerowego – o podjętej decyzji Centrum Techniczne SRnIK powiadamia organizatora systemu;
14) bierze udział w pracach grup roboczych w zakresie reagowania na incydenty komputerowe w systemach teleinformatycznych przeznaczonych do przetwarzania informacji jawnych lub narodowych informacji niejawnych;
15) informuje organizatora systemu o zdarzeniach, incydentach komputerowych, zagrożeniach związanych z monitorowanym systemem teleinformatycznym oraz o wydanych zaleceniach, podjętych decyzjach;
16) udziela niezbędnej pomocy pełnomocnikom do spraw ochrony informacji niejawnych w przypadku prowadzenia postępowania wyjaśniającego wystąpienie incydentu komputerowego;
17) udziela niezbędnej pomocy administratorom systemów teleinformatycznych w trakcie obsługi incydentu komputerowego oraz przywracania funkcjonowania systemu teleinformatycznego po zaistniałym incydencie;
18) utrzymuje laboratorium techniczne na potrzeby analizy kodów złośliwych oraz prowadzenia testów bezpieczeństwa i podatności;
19) prowadzi ewidencję administratorów systemów teleinformatycznych, zawierającą stopień wojskowy, imię i nazwisko oraz numer telefonu, nazwę

komórki albo jednostki organizacyjnej osoby wyznaczonej do pełnienia funkcji administratora systemu teleinformatycznego;

20) odpowiada za opracowanie i stałą aktualizację:

a) „Podręcznika reagowania na incydenty komputerowe w resorcie obrony narodowej”,

b) „Standardowych Procedur Operacyjnych SRnIK w resorcie obrony narodowej”;

c) „Wytycznych do opracowania Lokalnych Procedur Operacyjnych SRnIK w jednostce organizacyjnej”.

6. Administratorzy systemów teleinformatycznych w komórkach i jednostkach organizacyjnych są zobowiązani do:

1) wykonywania zaleceń Centrum Technicznego SRnIK w zakresie przeciwdziałania naruszeniom polityk bezpieczeństwa i obsługi incydentów komputerowych zgodnie z procedurami SRnIK;

2) wdrożenia w uzgodnieniu z kierownikiem jednostki organizacyjnej "Lokalnych Procedur Operacyjnych SRnIK w jednostce organizacyjnej" ujętych w dokumentacji bezpieczeństwa;

3) nadzorowania użytkowników administrowanych przez nich jawnych systemów teleinformatycznych oraz wspomagania inspektorów bezpieczeństwa teleinformatycznego w nadzorowaniu użytkowników administrowanych przez nich niejawnych systemów teleinformatycznych w zakresie przestrzegania ustalonych procedur bezpieczeństwa;

4) współpracy z instytucjami określonymi w pkt 5 ppkt 3 lit b-d w zakresie zabezpieczenia śladów i ustalenia przyczyn wystąpienia incydentu komputerowego, zgodnie z procedurami SRnIK;

5) zgłaszania do Centrum Technicznego SRnIK, a w przypadku systemów teleinformatycznych przetwarzających informacje niejawne dodatkowo do inspektora bezpieczeństwa teleinformatycznego, wykrytych incydentów komputerowych oraz wszelkich zdarzeń mogących wpłynąć na naruszenie polityki bezpieczeństwa w administrowanych przez nich systemach teleinformatycznych;

6) przesyłania niezwłocznie do Centrum Technicznego SRnIK wskazanych przez niego próbek kodu lub materiałów umożliwiających prowadzenia analiz technicznych, zgodnie z procedurami SRnIK, a w przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, na zasadach opisanych w dokumentacji bezpieczeństwa teleinformatycznego;

7) informowania Centrum Technicznego SRnIK przez kierownika jednostki organizacyjnej o zmianach personalnych administratorów systemów teleinformatycznych.

7. Dokumenty, o których mowa w pkt 5 ppkt 20, przed zatwierdzeniem przez Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni podlegają uzgodnieniu z:
   1) Departamentem Ochrony Informacji Niejawnych;
   2) Żandarmerią Wojskową;
   3) Centrum Koordynacyjnym SRnIK;
   4) Organizatorem Systemu Funkcjonalnego Wsparcia Dowodzenia;
   5) organizatorem systemu, w części dotyczącej jego systemu;
   6) Departamentem Strategii i Planowania Obronnego, w zakresie zachowania spójności dokumentów z Planem Zarządzania Kryzysowego MON, Wykazem przedsięwzięć i procedur systemu zarządzania kryzysowego oraz Planem Operacyjnym Funkcjonowania Działu Administracji Rządowej Obrona Narodowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny;
   7) Służbą Kontrwywiadu Wojskowego.
8. Kierownicy komórek i jednostek organizacyjnych zapewnią:
   1) możliwość realizacji zadań przez pełnomocników ochrony, inspektorów bezpieczeństwa teleinformatycznego i administratorów systemów teleinformatycznych zgodnie z określonymi procedurami;
   2) przestrzeganie obowiązujących dokumentów normatywnych i zaleceń w zakresie reagowania na incydenty komputerowe;
   3) realizowanie Lokalnych Procedur Operacyjnych SRnIK;
   4) nie później niż do końca 2015 r. uwzględnienie obowiązków nałożonych decyzją w dokumentacji bezpieczeństwa teleinformatycznego oraz dokumentacji eksploatacyjnej i procedurach dla systemów teleinformatycznych.
9. Traci moc decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. Min. Obr. Nar. Nr. 16, poz. 205).
10. Decyzja wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*