

Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP

Dokument przyjęty przez Zespół Zadaniowy ds. bezpieczeństwa cyberprzestrzeni
Rzeczypospolitej Polskiej i zatwierdzony przez Komitet Rady Ministrów ds. Cyfryzacji



Warszawa, 13 kwietnia 2015 roku

Plan działań w zakresie zapewniania bezpieczeństwa cyberprzestrzeni RP stanowi rekomendacje w zakresie bezpieczeństwa cyberprzestrzeni dla całej administracji publicznej. Dokument został opracowany i zarekomendowany przez Grupę Ekspertką, przyjęty przez Zespół Zadaniowy ds. bezpieczeństwa cyberprzestrzeni RP na posiedzeniu 20 marca 2015 roku, a następnie zatwierdzony w trybie obiegowym przez Komitet Rady Ministrów ds. Cyfryzacji.

Podstawę do opracowania *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP* stanowi *Polityka Ochrony Cyberprzestrzeni RP*, przyjęta przez Radę Ministrów 25 czerwca 2013 roku. Zgodnie z zapisami punktu 1.5. rzeczonego dokumentu, minister właściwy do spraw cyfryzacji odpowiada za koordynację założeń przyjętych w *Polityce*.

Wyjaśnienie skrótów: S – działania systemowe, I – działania w obrębie poszczególnych instytucji

DZIAŁANIA KRÓTKOTERMINOWE			
Perspektywa czasowa 3 miesiące			
		Proponowane działania	Instytucja odpowiedzialna
1.	S	Opracowanie założeń do nowej metodyki szacowania ryzyka	MAC – podmiot koordynujący Grupa Ekspercka – wsparcie merytoryczne
2.	S	Stworzenie rekomendacji co do posiadanych kwalifikacji osób zatrudnianych do zespołów reagowania na incydenty komputerowe	MAC – podmiot koordynujący Grupa Ekspercka – wsparcie merytoryczne
3.	S	Aktualizacja listy pełnomocników ds. bezpieczeństwa cyberprzestrzeni	MAC – podmiot koordynujący
4.	I	Powołanie pełnomocnika ds. bezpieczeństwa cyberprzestrzeni i przekazanie informacji na ten temat do MAC (W celu usprawnienia komunikacji zaleca się utworzenie ogólnego adresu „pełnomocnikBC_nazwa instytucji”, przypisanego do funkcji pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, a nie do konkretnej osoby)	MAC – podmiot koordynujący Każda instytucja
5.	I	Powołanie przez instytucje lokalnych zespołów reagowania na incydenty komputerowe lub przypisanie funkcji reagowania na incydenty komputerowe do istniejącej już komórki oraz zapewnienie skutecznej formy wymiany informacji z CERT.GOV.PL (W celu zapewnienia skutecznej komunikacji pomiędzy instytucją a CERT.GOV.PL zaleca się przekazanie do CERTu numeru telefonu/ faxu oraz dwóch adresów mailowych, w tym jednego podstawowego w formacie wskazującym na CERT oraz nazwę instytucji)	Każda instytucja Przekazanie informacji do CERT.GOV.PL i MAC
Perspektywa czasowa 6 miesięcy			
6.	S	Wypracowanie jednolitej terminologii i taksonomii w dziedzinie cyberbezpieczeństwa	MAC – podmiot koordynujący CERT.GOV.PL, RCB, MON, NASK, BBN – wsparcie merytoryczne
7.	S	Opracowanie nowej metodyki szacowania ryzyka	MAC – podmiot koordynujący
8.	S	Szkolenia dla jednostek z nowej metodyki szacowania ryzyka	MAC – podmiot koordynujący
9.	S	Opracowanie planu założeń do ustawy regulującej system cyberbezpieczeństwa RP (implementacja dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego poziomu bezpieczeństwa sieci i informacji w obrębie Unii tzw. NIS – <i>network and information security</i> , ang. Directive concerning measures to ensure a high common level of network and information security across	MAC – podmiot koordynujący

		the Union; ustanowienie CERTU narodowego; określenie jasnych kompetencji istniejących CERTów; określenie kompetencji i zadań w dziedzinie cyberbezpieczeństwa dla konkretnych instytucji)	
10.	S	Opracowanie rekomendacji mających na celu podnoszenie bezpieczeństwa systemu teleinformatycznego dla administracji publicznej w obszarze wymagań technicznych	CERT.GOV.PL – podmiot wiodący NASK, MON, RCB, MAC – podmioty wspierające
11.	S	Oszacowanie kosztów realizowanych zadań z zakresu bezpieczeństwa cyberprzestrzeni zgodnie z pkt 5 Polityki Ochrony Cyberprzestrzeni i przekazanie do MAiC corocznie do 31 stycznia (Zadanie do realizacji począwszy od 2016 r)	Ministerstwo Finansów – podmioty wiodący Każda instytucja
12.	I	Wprowadzenie w instytucjach procedury reagowania na incydenty, określającej zasady i formy zgłaszania wystąpienia incydentu przez pracowników. Procedura powinna zawierać: - Zasady i sposób zgłaszania przez pracowników podejrzenia wystąpienia incydentu IT- Funkcjonującą w instytucji procedurę reagowania na incydenty wraz z ujęciem współpracy z właściwym Zespołem CERT (obecnie: CERT.GOV.PL, CERT.PL, SRnIK) - Przekazywanie informacji o wystąpieniu incydentu i stwierdzonych podatnościach występujących w instytucjach do właściwego CERTu	Każda instytucja
13.	I	Przygotowanie planów przywrócenia ciągłości działania w stosunku do jawnych systemów IT, oraz późniejsza coroczna ich aktualizacja	Każda instytucja
DZIAŁANIA DŁUGOTERMINOWE			
14.	S	Opracowanie założeń do ustawy regulującej system cyberbezpieczeństwa RP (implementacja dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego poziomu bezpieczeństwa sieci i informacji w obrębie Unii tzw. NIS – <i>Network and Information Security</i> ; ustanowienie CERTU narodowego; określenie jasnych kompetencji istniejących CERTów; określenie kompetencji i zadań w dziedzinie cyberbezpieczeństwa dla konkretnych instytucji)	MAC – podmiot koordynujący
15.	S	Doprowadzenie do sytuacji w której wyniki oceny ryzyka sporządzonej na potrzeby <i>Polityki Ochrony Cyberprzestrzeni RP</i> byłyby możliwe do wykorzystania w ramach oceny sporządzonej na potrzeby <i>Raportu o zagrożeniach bezpieczeństwa narodowego</i> poprzez zapewnienie spójności obu metodyk	RCB, MAC – podmioty wiodące BBN – konsultacje merytoryczne Administracja rządowa – podmioty wspierające
16.	S	Ustalenie procesów zarządzania kryzysowego w obliczu zagrożenia cybernetycznego oraz koordynacja <i>Krajowego System Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej</i> z regulacjami dotyczącymi wprowadzania stanów nadzwyczajnych	MAC, RCB – podmioty wiodące BBN – konsultacje merytoryczne Grupa Ekspercka, Administracja rządowa – podmioty wspierające

		Określenie rodzajów oraz skali incydentów upoważniających do wprowadzenia, wymienionych w art. 228 ust. 1 Konstytucji RP, stanów nadzwyczajnych, tj. stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej	
17.	S	Zaplanowanie i uruchomienie cyklicznych ćwiczeń międzyresortowych, związanych z bezpieczeństwem cyberprzestrzeni Ćwiczenia powinny mieć formę symulacji wystąpienia zagrożeń dla systemów teleinformatycznych i angażować zarówno jednostki administracji rządowej, jak i służby wspierające je w zarządzaniu incydentami	RCB, MAC – podmioty wiodące ABW (CERT.GOV.PL) – podmiot wspierający
18.	S	Prowadzenie i rozwój portalu ułatwiającego producentom treści edukacyjnych wymianę treści merytorycznych (w zakresie cyberbezpieczeństwa), a także tworzenie materiałów dostosowanych do potrzeb i profilu własnego odbiorcy (w tym np. tłumaczenie informacji z innych krajów) oraz publikowanie ich lokalnie, przede wszystkim na potrzeby użytkowników domowych oraz małych i średnich przedsiębiorstw	NASK
19.	S	Prowadzenie forum internetowego poświęconego zwalczaniu nadużyć w sieci	NASK
20.	S	Współpraca z uczelniami mająca na celu promocję treści z zakresu bezpieczeństwa teleinformatycznego oraz zachęcanie do wprowadzenia do programów nauczania, na odpowiednich kierunkach kształcenia tych treści	MNiSW – podmiot wiodący Polska Komisja Akredytacyjna, rektorzy wyższych uczelni, MAC – podmioty wspierające
21.	S	Utrzymanie w szkolnych programach nauczania (w ramach lekcji z zakresu technologii informacyjnych) bloku zajęć realizującego zagadnienia dot. cyberbezpieczeństwa	MEN – instytucja wiodąca
22.	S	Gromadzenie i udostępnianie e-zasobów edukacyjnych z zakresu istoty i profilaktyki cyberprzemocy w bibliotekach szkolnych i pedagogicznych oraz na stronach internetowych instytucji oświatowych (ORE, dyrektorzy szkół i dyrektorzy bibliotek pedagogicznych, dyrektorzy ośrodków doskonalenia nauczycieli)	MEN – podmiot wiodący Wykorzystanie portalu Scholaris
23.	S	Organizacja współpracy szkół z lokalnymi jednostkami policji i instytucjami wymiaru sprawiedliwości oraz operatorami telekomunikacyjnymi w zakresie edukacji uczniów i rodziców z tematyki ochrony dzieci i młodzieży przed zagrożeniami z Internetu	MEN – podmiot koordynujący
24.	S	Rozbudowanie oferty szkoleń dla nauczycieli o tematykę cyberbezpieczeństwa	MEN Ośrodki Doskonalenia Nauczycieli
25.	S	Współpraca z uczelniami w kreowaniu i promocji kierunków kształcących specjalistów w dziedzinie bezpieczeństwa cyberprzestrzeni	MNiSW – podmiot wiodący MAC – podmiot wspierający
26.	S	Rozwój narzędzi teleinformatycznych dla administracji, wspierających ochronę kluczowych systemów – m.in. rozwój systemu ARAKIS-GOV	ABW (CERT.GOV.PL), NASK – podmioty wiodące
27.	I	Opracowanie i wprowadzenie przez instytucje Polityki Bezpieczeństwa Informacji	Każda instytucja
DZIAŁANIA CIĄGŁE			

28.	S	Przygotowywanie rocznych raportów zawierających zanonimizowane dane statystyczne dotyczące zgłoszonych incydentów (w przypadku UKE zgodnie z zapisami art 175 b ust 4 Prawa Telekomunikacyjnego), oraz przekazanie właściwemu ministrowi ds. informatyzacji (UKE minister właściwy ds. łączności) – coroczne w terminie do 30 kwietnia	Właściwe CERTy, UKE
29.	S	Szkolenia dla pełnomocników ds. bezpieczeństwa cyberprzestrzeni	MAC
30.	S	Analiza pojawiających się nowych zagrożeń i ich wpływu na bezpieczeństwo jawnych systemów IT administracji rządowej	Właściwe CERTy
31.	I	Szacowanie ryzyka związanego z przetwarzanymi informacjami w systemach informatycznych oraz sporządzanie sprawozdania z jego wykonania Corocznie do 31 stycznia (podstawa: pkt.3.1. <i>Polityki ochrony cyberprzestrzeni RP</i>)	Właściwy Minister lub Prezes instytucji (Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni instytucji we współpracy z kierownikami komórek operacyjnych)
32.	I	Szacowanie ryzyka w portalach internetowych oraz sporządzenie sprawozdania z jego wykonania Corocznie do 31 stycznia (podstawa: pkt. 3.2. <i>Polityki ochrony cyberprzestrzeni RP</i>)	Właściwy Minister lub Prezes instytucji (Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni instytucji we współpracy z kierownikami komórek operacyjnych)
33.	I	Szkolenia dla wszystkich pracowników instytucji z zakresu bezpieczeństwa teleinformatycznego	Każda instytucja
34.	I	Szkolenie nowo przyjętych pracowników z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego, funkcjonującego w obrębie danej organizacji	Każda instytucja