Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

§ 1

Postanowienia ogólne

1. „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem” (zwana dalej „Procedurą”) ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływów przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność podmiotu.
2. Podstawą prawną do opracowania i wdrożenia procedury jest:
   1) art. 22 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
   2) § 20 ust. 2 pkt. 13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
   3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

§ 2

Kategorie incydentów

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną mogą być:
   1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
   2) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
   3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
2. Incydentami bezpieczeństwa informacji w szczególności są:
   1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
   1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
   2) działania szkodliwego oprogramowania;
   3) próby omijania systemów zabezpieczeń;
   4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   6) zniszczenia lub kradzieży nośników danych;
   7) prób wyłudzeń informacji;
   8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
   9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych.
4. Za incydent poważny uznaje się zdarzenie, które spowodowało lub mogło spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla ADO lub wpłynęło lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.

§ 3

Przykładowe zdarzenia które mogą być zakwalifikowane jako podejrzenie naruszenia bezpieczeństwa informacji

1. Za przykładowe zdarzenia, które mogą być zakwalifikowane jako podejrzenie naruszenia bezpieczeństwa informacji można uznać np.:
   1) Awarię sprzętu lub oprogramowania, które wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
   2) Nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: pożar, zalanie pomieszczeń, zerwanie linii wysokiego napięcia, niepożądana ingerencja firmy remontowej itp.;
   3) Nieodpowiednie warunki środowiskowe panujące w serwerowni takie jak zbyt wysoka temperatura lub nadmierna wilgotność;
   4) Wystąpienie nieautoryzowanej manipulacji danymi w systemie;
   5) Praca w systemie osób niedopuszczonych do jego obsługi;
   6) Ujawnianie nieupoważnionym osobom danych osobowych lub objętych tajemnicą elementów systemu zabezpieczeń;
   7) Wystąpienie nieprawidłowości związanych z przechowywania danych, w tym osobowych np. pozostawienie otwartych szaf, biurek itp.

§ 4

Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie ADO, ASI oraz IOD.
2. Jednocześnie wskazuje się, że IOD został przez ADO wyznaczony jako osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w związku z realizacją zadań wynikających z art. 22-24 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
3. Zgłoszenia dokonuje się telefonicznie lub osobiście.
4. Zgłoszenie należy potwierdzić szczegółową notatką służbową.
5. Notatka powinna zawierać następujące informacje:
   1) imię i nazwisko zgłaszającego;
   2) stanowisko;
   3) dokładne miejsce oraz datę wystąpienia incydentu;
   4) opis incydentów sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego;
   5) opis wyrządzonych szkód majątkowych i/lub niemajątkowych w związku z wystąpieniem incydentu;
   6) źródło wystąpienia incydentu (np. niedbalstwo, umyślność);
   7) podjęte działania naprawcze i/lub korygujące;
   8) inne okoliczności łagodzące i/lub obciążające.
6. Brak umiejętności poprawnego rozpoznania incydentu przez osobą zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
7. W przypadku nieobecności IOD lub ASI incydent należy zgłosić do ADO lub osoby wskazanej przez ADO.

§ 5

Postepowanie z incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez IOD oraz ASI i przechowywane w dokumentach IOD.
2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
3. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia.
4. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, IOD oraz ASI dokonuje jego oceny istotności.
5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   1) powstałe szkody będące wynikiem incydentu;
   2) wpływ incydentu na działanie systemów;
   3) wpływ incydentu na ciągłość działania;
   4) koszty usunięcia skutków incydentu;
   5) szacowany czas naprawy skutków wywołanych incydentem;
   6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów;
   7) znaczenie incydentu dla świadczenia usług danego podmiotu;
   8) dotkliwość i charakterystykę techniczną cyberzagrożenia;

9) bazowe podatności, które są wykorzystywane;
10) doświadczenie z podobnymi incydentami;
11) czas trwania incydentu;
12) liczba dotkniętych nim odbiorców usług.

6. Zakwalifikowanie zgłoszenia jako „fałszywy alarm” kończy postępowanie.
7. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI wespół z IOD podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku stwierdzenia incydentu poważnego, ADO bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o poważnym incydencie dokonuje wczesnego ostrzeżenia, w którym w stosownych przypadkach wskazuje, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny. Organem właściwym do przyjęcia wczesnego ostrzeżenia jest CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy ul. Kolska 12, 01-045 Warszawa). ADO nie później niż w ciągu 72 godzin od momentu wykrycia incydentu poważnego, zgłasza aktualizację do właściwego CSIRT NASK ujmując takie informacje jak: dotkliwość incydentu, skutki incydentu, a w stosowanych przypadkach również informacje dotyczące wskaźników integralności systemu. ADO przekazuje, na wniosek CSIRT NASK sprawozdanie okresowe z obsługi incydentu poważnego i przekazuje także CSIRT NASK sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu poważnego.
9. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. W przypadku braku możliwości przekazania zgłoszenia w sposób elektroniczny należy dokonać go przy użyciu innych dostępnych środków komunikacji tj. telefon, fax.
10. W zgłoszeniu przekazuje się informacje zgodne z formularzem oraz zgodnie z wymogami art. 23 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz art. 23 Dyrektywy NIS2.
11. W przypadku zaistnienia znaczącego cyberzagrożenia, które może wpłynąć na świadczone usługi, ADO informuje swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. ADO informuje tych użytkowników o samym znaczącym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.
12. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie w zależności od wagi incydentu może powiadomić organy ścigania.
13. W przypadku, kiedy incydent ma charakter naruszenia, o którym mowa w art. 33 i/lub 34 RODO, stosuje się dodatkowo procedury określone w ramach Polityki Ochrony Danych (rozdział: „Procedura zarządzania naruszeniami”).

§ 6

Szkolenia

W celu zwiększenia wśród pracowników umiejętności poprawnego rozpoznania i klasyfikacji incydentów zaleca się, co najmniej raz do roku przeprowadzać okresowe szkolenie pracowników w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowo zatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.