Załącznik nr 1 do Zarządzenia nr 20/2024
Dyrektora Powiatowego Urzędu Pracy w Bytowie
z dnia 17 października 2024 r.

Procedura zarządzaniem incydentem w podmiocie publicznym

I. Postanowienia ogólne

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Powiatowego Urzędu Pracy w Bytowie.

II. Incydent w podmiocie publicznym

1. Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych;
2. Incydentami 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;
   4) naruszenie autentyczności, to jest braku wiarygodności danych.
3. Przyczyny incydentów bezpieczeństwa informacji mogą dotyczyć:
   1) niewłaściwego wykorzystywania zasobów informatycznych;
   2) działania szkodliwego oprogramowania;
   3) próby omijania systemów zabezpieczeń;
   4) nieautoryzowanego dostępu do systemów, aplikacji;
   5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
   6) zniszczenia lub kradzieży nośników danych;
   7) próby wyłudzeń informacji;
   8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
   9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych;
   10) naruszenia obowiązujących w Powiatowym Urzędzie Pracy w Bytowie zasad dotyczących bezpieczeństwa informacji.

III. Zgłaszanie incydentów związanych z bezpieczeństwem informacji

1. Naruszenie bezpieczeństwa zasobów informacyjnych musi być zgłaszane przez pracowników Powiatowego Urzędu Pracy w Bytowie. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy i umiejętności. Zgłoszenie incydentu musi być przekazane Administratorowi Systemu Informatycznego (ASI). Zgłoszenie powinno być przekazane telefonicznie i potwierdzone w formie elektronicznej.
2. Zgłoszenie musi zawierać następujące informacje:
   1) imię i nazwisko osoby zgłaszającej,
   2) miejsce i datę wystąpienia incydentu,

3) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

IV. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowanie jest przez ASI w rejestrze incydentów związanych z cyberbezpieczeństwem (załącznik nr 1 do niniejszej procedury). ASI zabezpiecza materiał dowodowy (np. zrzut ekranu monitora, logi systemu itp). Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji, dokonywana jest jego ocena istotności. Powyższe działania wykonuje IOD w porozumieniu z ASI.
2. 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 urzędu;
   4) koszty usunięcia skutków incydentu;
   5) szacowany czas naprawy skutków wywołanych incydentem;
   6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym ASI informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji, IOD wraz z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. W przypadku, gdy waga incydentu dotyczy systemów informatycznych i zakwalifikowana jest jako **wysoka**, o incydencje zawiadamiany jest zespół reagowania na incydenty CERT Polska – działający w strukturach Naukowej i Akademickiej Sieci Komputerowej – NASK (zgodnie z informacją zamieszoną na stronie www.cert.pl). Działania te podejmuje ASI.
6. O wynikach analizy incydentu oraz podjętych działaniach naprawczych ASI informuje Administratora Danych.
7. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji Administrator Danych podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być zawiadomione organa ścigania.
8. Powyższe działania raportowane są w rejestrze incydentów związanych z cyberbezpieczeństwem.

Signed by / Podpisano przez:

Janusz Wiczkowski

Date / Data: 2024-10-17 14:42