Załącznik nr 4
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji

WYDANIE - 1

Wersja – 1

Spis treści

1. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest zapewnienie że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

2. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich wydziałach, biurach i pozostałych komórkach organizacyjnych Urzędu oraz innych jednostkach korzystających z sieci komputerowej Urzędu. Niniejsza procedura jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w Urzędzie.

3. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach Urzędu dokonujących zgłoszeń. Każdy pracownik Oddziału ds. Informatyki odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.

Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji jest odpowiedzialny za:

1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;
4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie;
7) Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

4. Klasyfikacja incydentów.

Podział zdarzeń:

1) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zdarzenia zamierzone, świadome i celowe – stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
   - nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do danych z sieci wewnętrznej,
   - nieuprawniony transfer danych,
   - pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
   - bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.

12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

5. Zgłaszanie incydentów

Pracownicy Urzędu mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem. **Punktem kontaktowym jest Oddział ds. Informatyki. Incydenty można zgłaszać na portalu dla pracowników na mac0 w formularzu do zgłaszania awarii, mailem do Kierownika Oddziału ds. Informatyki lub telefonicznie pod numery 13-80, 17-52, 18-51**. Zgłoszenie musi zawierać:

- imię i nazwisko zgłaszającego,
- miejsce i datę wystąpienia incydentu,
- opis zdarzenia.

Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia istnienia wirusa komputerowego należy postępować zgodnie z Instrukcją w zakresie profilaktyki antywirusowej, zał nr 6 do PBI.

6. Postępowanie z incydentami

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.

1) Pracownik Oddziału ds. Informatyki , który przyjął zgłoszenie, powiadamia niezwłocznie kierownika oddziału lub osobę go zastępującą o fakcie i treści zgłoszenia.
2) Po analizie zdarzenia i okoliczności z nim związanych Kierownik Oddziału ds. Informatyki wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy. Zawiadamia członków Zespołu ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji.
3) Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego:

- dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony
- dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

4) W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent bezpieczeństwa informacji, Zespół dokonuje oceny istotności incydentu oraz zawiadamia Dyrektora Generalnego Urzędu o zaistnieniu incydentu oraz poziomie zagrożenia dla bezpieczeństwa informacji. Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji ocenia poziom istotności incydentu dla Urzędu kierując się następującymi kryteriami:
   - wpływ incydentu na ciągłość działania Urzędu i wypełnianie jego zadań statutowych;
   - krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
   - wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej – np.: danych osobowych, informacji niejawnych);
   - rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć itp.);
   - rozmiar szkód powstałych skutkiem incydentu;
   - koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
   - szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
   - zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych itp.);

5) Jeżeli istotność incydentu jest wysoka, należy zawiadomić Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełniący rolę głównego zespołu CERT w obszarze administracji rządowej. Wyznaczony przez przewodniczącego członek zespołu wypełnia formularz zgłoszenia incydentu, ściągnięty ze strony www.cert.gov.pl oraz wysyła go do CERT zgodnie z informacją zamieszczoną na tej stronie. Incydent zgłaszany jest dwutorowo, faksem na numer +48 22 58 58 833 oraz pocztą elektroniczną na adres incydent@cert.gov.pl . Dalsza korespondencja z CERT w sprawie tego incydentu odbywa się za pomocą szyfrowanej poczty elektronicznej.
6) W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ma charakter fałszywego alarmu Kierownik Oddziału ds. Informatyki powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydent bezpieczeństwa.
7) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym Dyrektorowi

Generalnemu w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

8) Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.
9) Zespół na bieżąco dokumentuje swoje działania na każdym z etapów procesu zarządzania incydentem w formie notatki. Obsługa incydentu kończy się raportem zatwierdzonym przez Przewodniczącego Zespołu zawierającym opis incydentu oraz wnioski co do działań na przyszłość.

7. Szkolenia.

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz do roku należy przeprowadzać okresowe szkolenia pracowników Urzędu w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

Schemat postępowania z incydentami związanymi z bezpieczeństwem informacji